DLAM 5200.08

DEFENSE LOGISTICS AGENCY

AMERICA'S COMBAT LOGISTICS SUPPORT AGENCY

PHYSICAL SECURITY MANUAL 2011

Issue Date: December 2, 2011 OPR: DLA Installation Support, Security & Emergency Services
Updated: Certified Current, January 30, 2014 Next Review:

Table of Contents

PREFACE

I. PURPOSE.

A. General. This Manual supplements processes and procedures outlined in Defense Logistics Agency Instruction (DLAI) 4306, *Physical Security Program* and joint regulations AR 190-16/OPNAVINST 5530.15A/AFR 207-4/MCO 5500.13A/DLAR 5710.4. It is directive in nature. It implements Department of Defense (DoD) 5200.8-R, *Physical Security Program.* It prescribes procedures and minimum standards for the physical protection of DLA personnel, installations, activities and separate facilities, operations, and assets. This DLA Manual is issued in accordance with the requirements of DoD Directive 5200.8, *Security of DoD Installations and Resources and the Physical Security Review Board (PSRB).*

B. Overview. This Physical Security Manual provides a compact source of basic information to assist PLFA Commanders/Directors, Installation Commanders, Depot Commanders, Site Directors, managers, designated officials, property officers, and security personnel in understanding and establishing appropriate physical security measures necessary to protect personnel, real and personal property, resources, and information. No information contained in the manual is intended to alter any provision of any Federal law, Executive Order, or national or DoD directive.

C. Restrictions. This manual does not pertain to the construction standards of Sensitive Compartmented Information Facilities, Special Access Program Facilities and Communications Security vaults. For regulatory guidance on the aforementioned areas, refer to the appropriate directive, instruction, regulation and any other guidance applicable to those areas.

II. APPLICABILITY, SCOPE AND OBJECTIVES.

A. Applicability and Scope.

This manual implements the DLA Physical Security Program. It establishes and implements processes and procedures necessary for effective, efficient, and economical conduct of official Agency business. It applies to active duty military personnel, reserve duty military personnel, DoD civilians, and to contractors and their employees as required by binding agreement or obligation (Government Contract, Memorandum of Agreement/Understanding or Inter Agency Service Agreement) with DLA. The terms "must," "shall," and "will" denote mandatory actions in this manual. In cases where this would conflict with other regulations or policies, an agreement between the tenant and host will be coordinated by the PLFA Commander/Director. When DLA is a tenant, that activity shall abide by the Host Installation requirements in accordance with ISSA(s), MOA(s) and/or MOU(s). When a particular requirement imposed by this manual is not addressed or required by the Host Installation, then that activity will comply with this manual as long as it does not violate any ISSA(s), MOU(s) and/or MOA(s) the activity has with the Installation.

Note: When operations unique to an activity necessitate a divergence from the requirements of this Manual, the threat, operating environment and conditions shall be evaluated to tailor the security requirements of this Manual to include compensatory measures implemented. The security requirements shall be based on risk management, practicality, cost, and mission performance. In these instances, waivers, variances and exceptions to the requirements of this Manual shall be submitted according to the provisions in Chapter 17 of this Manual.

B. Objectives.

1. Implement general policy for the security of personnel, installations, military operations, and certain additional assets.

2. Provide security guidance and general procedures that are realistic, harmonized with other security disciplines, and provide the necessary flexibility for PLFA Commanders/Directors, Installation Commanders, and Depot Commanders to protect personnel, installations, projects, operations, and related resources against capable threats from terrorists, criminal activity, and other subversive or illegal activity.

3. Reduce the loss, theft, diversion of, or damage to DoD assets through the use of advanced technologies; thereby enhancing overall security, while ensuring that the warfighting capability is maintained.

4. Personal identification and authentication to DoD installations and facilities, including interoperability with other Federal entities, utilizing the DoD Personal Identity Verification (PIV) credential (Common Access Card (CAC)) as the universal authority of individual authenticity, *consistent with applicable law*. The DoD PIV credential will provide the Homeland Security Presidential (HSPD)-12 mandated level of identity assurance and government-wide recognition.

III. RESPONSIBILITIES.

A. HQ DLA. The Staff Director, Security and Emergency Services.

1. Develops and prescribes general physical security requirements and ensures HQ DLA staff supervision of the DLA Physical Security Program.

2. Conducts staff assistance visits and inspections of DLA Activities. The purpose of these visits is to assist DLA Activities in achieving compliance with the provisions of this and other physical security regulations and to assess the applicability and effectiveness of those regulations.

3. Sponsors programs and measures with other Government agencies that will contribute to the ultimate objectives of the DLA Physical Security Program.

B. DLA Primary Level Field Activities (PLFA).

1. DLA PLFA Commanders/Directors shall:

a. Have responsibility for the safety of personnel and protection of Federal property under their control.

b. Be responsible for the implementation of physical security measures designed to minimize the loss of supplies and equipment by natural or manmade hazards.

c. Ensure the organization of their activity includes a Chief, Security and Emergency Services/Chief, Security Services and organizational placement of this individual does not hinder accomplishment of the security mission.

2. The Chief, Security and Emergency Services/ Chief, Security Services at each PLFA will:

a. Administer the activity's physical security program.

b. Assist the PLFA Commander/Director, Site Director, leadership and supervisors in discharging their security responsibilities by analyzing security deficiencies and hazards and making recommendations for appropriate corrective action.

c. Ensure physical security inspections are conducted annually. In addition, where applicable, conduct surveys and exercises of DLA restricted and controlled areas, facilities storing arms, ammunition, and explosives (AA&E), and other facilities storing sensitive or pilferable resources as outlined in this manual.

d. Direct and control the training and utilization of the activity's security forces personnel.

e. Review security reports and logs on a daily basis to ensure compliance with established security procedures.

f. Appoint in writing a physical security specialist to manage the physical security program.

IV. SUGGESTED IMPROVEMENTS.

Users are invited to send comments and suggested improvements directly to HQ DLA, Security and Emergency Services, 8725 John J. Kingman Road, Suite 3533, Fort Belvoir, VA 22060-6220.

V. EFFECTIVE DATE AND IMPLEMENTATION.

This manual supersedes the DLA Physical Security Guidebook and is effective immediately.

Approved

Director, DLA Strategic Plans and Policy

CHAPTER 1: PHYSICAL SECURITY PLANNING

A. General.

1. Physical security is that portion of security concerned with procedures and physical measures designed to safeguard personnel, property, and operations; to prevent unauthorized access to equipment, facilities, material, and information; and to protect against espionage, terrorism, sabotage, damage, misuse, and theft.

a. Physical security procedures include, but are not limited to, the application of physical measures to reduce vulnerability to the threat; integration of physical security into contingency, mobilization, and wartime plans; the testing of physical security procedures and measures during the exercise of these plans; the interface of installation OPSEC, crime prevention and physical security programs to protect against the traditional criminal; training of security forces in tactical defense against and response to attempted penetrations; and creating physical security awareness.

b. Physical security measures are physical systems, devices, personnel, animals, and procedures employed to protect security interests from possible threats and include, but are not limited to, security guards; military working dogs; lights and physical barriers; explosives and bomb detection equipment; protective vests and similar equipment; badging systems; electronic entry control systems and access control devices; security containers; locking devices; electronic intrusion detection systems; standardized command, control, and display subsystems; radio frequency data links used for physical security; security lighting; delay devices; biometrics; and assessment and/or surveillance systems to include closed-circuit television. Depending on the circumstances of the particular situation, security specialists may have an interest in other items of equipment such as armored sedans.

2. Many regulations specify protective measures, policies, and operations related to security. Physical, personnel, antiterrorism (AT), force protection, law enforcement, operations, communications and information security programs and surveys are all vital components of a total security system and must be effectively integrated to provide in-depth protection.

3. An activity Physical Security Program will include, at a minimum, the following functions:

a. Implementation of physical protective measures and operational procedures designed to safeguard personnel and protect DLA resources from unauthorized use, theft, damage, sabotage, and espionage.

b. Development of site-specific procedures in concert with higher HQ regulations to enhance security at specific activities.

c. Inspection of all areas to ensure compliance with higher HQ directives and activity procedures.

d. Implementation and management of a Physical Security Education and Training Program for all activity employees.

e. Implementation and management of loss prevention procedures to identify loss trends and detect criminal activity.

f. Where applicable, management and utilization of DLA police.

4. This manual addresses minimum security standards and procedures for DLA. DLA activities will maintain flexibility in planning and in determining the degree of protection and the scope of the Physical Security Program, commensurate with the mission.

B. Planning Considerations.

1. In determining the type and extent of physical protection required at an activity, a risk management and analysis approach shall be used. Prime consideration will be given to the activity's operational requirements. The following factors should be considered:

a. Mission - What is the importance of the activity to the continuing mission of DLA?;

b. Areas to be protected;

c. Local threats and vulnerabilities;

d. Impact of physical security measures on efficiency of operations;

e. Costs of material and equipment to be installed and availability of funds;

f. Potential damage or loss to the activity, to DLA and/or to the DoD;

g. Alternate security measures or techniques;

h. Security, AT, and force protection standards directed by higher headquarters.

2. Each activity must continually evaluate its security posture in light of the factors above and then devise appropriate physical security measures. When evaluating the degree and type of physical security required, planners must remember that the criticality of an activity may vary as its products or services become more or less important to the mission of DLA.

3. During planning, consider standards and procedures for the following:

a. Education of personnel in the use of internal control procedures and the need for vigilance to prevent losses;

b. Receiving stock, stock control, and shipping;

c. Receiving, holding, or banking money;

d. Storing and accounting for controlled items, including narcotics, AA&E, classified mission stock, and hazardous materials;

e. Structural criteria of buildings; (Use Unified Facilities Criteria)

f. Police or contract guard utilization;

g. Communications.

h. Installation and use of intrusion detection systems (IDS), card reader systems, automated key control systems, and other physical security equipment.

4. Activities will implement local procedures to ensure plans for all site improvements and major construction projects with security impact are reviewed and coordinated with the security office.

C. Physical Security Plan.

1. Each DLA installation/PLFA will develop a localized physical security plan to supplement this manual. The plan shall be fully integrated with Antiterrorism (AT) plans to ensure employment of a holistic security system to counter terrorist capabilities. Annexes to the plan may be separated for operational purposes as required; however, the location of the annexes will be listed in the plan. The physical security plan, including all annexes, shall be exercised annually in order to evaluate its effectiveness. As a minimum, the plan will include:

a. An installation/facility local threat statement;

b. An installation access control and closure plan;

c. Protective lighting plan;

d. A civil disturbance plan. It is the PLFA Commander's/Director's responsibility to formulate a civil disturbance plan based on local threats;

e. A resource plan to meet minimum essential physical security needs for the installation or activity;

f. A list of Installation /Activity Critical Assets;

g. Lists of designated Restricted and Controlled areas, areas assigned to a Resource Level (1, 2, or 3), and the associated Alarm Priority Response Lists (APRLs);

h. A contingency plan. Such contingencies may include hostage negotiations, active shooter response, protective services, and special reaction teams;

i. Annexes containing the installation/facility AT Plan and the Chemical, Biological, Radiological, Nuclear, and Explosive (CBRNE)/Hazardous Material (HAZMAT) Protection Plan.

2. Sample Plan. The sample plan outlined in Appendix C is one means of developing a Physical Security Plan. It is meant to help structure the local physical security plan in a comprehensive and organized manner.

D. Physical Security Funding:

DoD 7000.14-R, DoD Financial Management Regulation, Volume 2B, Chapter 19, provides instructions applicable to budget formulation for the DoD Combating Terrorism (CbT) funding requirements.

1. AT CbT subcategories include the following:

a. Physical Security Equipment;

b. Physical Security Site Improvements;

c. Physical Security Management and Planning;

d. Security Forces/Technicians;

e. Law Enforcement;

f. Security Matters;

g. Consequence Management.

2. Chiefs, Security and Emergency Services/Chiefs, Security Services will coordinate funding requests through activity budget analyst and DLA Installation Support, Office of Security and Emergency Services.

E. Security Executive Committee (SEC) and Security Working Groups (SWG).

The SEC and all his subordinate working groups will comply with DLA Instruction 4301, Security and Emergency Services, which provides specific requirements and responsibilities for the SEC. See Chapter 17, Working Groups for additional information and requirements.

F. Security Engineering.

1. The security engineering design process identifies assets requiring protection, determines the threat to and vulnerability of those assets, and designs a protective system to protect the assets.

2. A security engineering survey is the process of identifying, by means of an on–site survey, engineering requirements associated with facility enhancements for physical security and anti–terrorism, including intrusion detection system (IDS) installation. Using a team concept, security engineering surveys should be performed locally when planning any new construction or renovations or upgrades to existing facilities where there are likely to be physical security requirements. Security engineering surveys may also be requested by the Chiefs, Security and Emergency Services/Chiefs, Security Services to evaluate existing security.

3. The scope of a security engineering survey is to:

a. Identify the assets to be protected.

b. Identify the threats to the assets and the levels of protection to which the assets should be protected.

c. Identify protective measures, including IDS, to reduce the vulnerabilities of the assets to the threats.

d. Determine the cost of proposed protective measures.

4. As a minimum, the following personnel should make up the security engineering planning team:

a. Physical Security Specialist;

b. AT Officer;

c. Installation or Facility Engineer;

d. Intelligence Officer (if applicable);

e. Customer;

f. Logistics Officer;

g. Safety Officer;

h. Fire and Emergency Services;

i. Investigator (if applicable).

G. Physical Security and Operations Security (OPSEC).

OPSEC is an analytic process used to deny an adversary unclassified but sensitive information concerning our intentions and capabilities by identifying, controlling, and protecting indicators associated with our planning processes or operations. OPSEC does not replace physical security and other security disciplines - it supplements them.

1. The threat defines the physical security challenges.

2. Chiefs, Security and Emergency Services/Chiefs, Security Services must consider OPSEC in physical security planning and ensure OPSEC is implemented to support physical security measures. A few examples are, providing soundproof rooms for conducting briefings, not publicizing RAMS, security systems layouts, etc.

3. Chiefs, Security and Emergency Services/Chiefs, Security Services must work in concert with OPSEC personnel to ensure physical security critical information is included within the installation/activity Critical Information List.

4. For additional information refer to DoD 5205.02, *DoD Operations Security Program*, and DLA Instruction 6305, *Operations Security*. (http://www.dtic.mil/whs/directives/corres/pdf/520502p.pdf / https://headquarters.dla.mil/DES/policy/i6305.htm).

H. Security Deviations.

Activities must implement the security deviation program where resources are not protected at the required protection level. See DLA Instruction 4301, Security and Emergency Services and Chapter 16, Waivers, Variances, and Exceptions for additional information. If a conflict exists between this manual and any other DoD document, referenced code, standard, or publication, Unified Facilities Criteria (UFC) 3-600-01 (Fire Protection Engineering for Facilities) takes precedence.

CHAPTER 2: INSTALLATION ENTRY & INTERNAL CONTROL

A. General.

1. This chapter outlines procedures for installation entry and internal control of DLA installations and facilities. PLFA Commanders/Directors must establish installation entry and internal control procedures that comply with DoD and DLA policy.

2. Entry Controls. These procedures are designed to deter unauthorized entry and counter the introduction of hazardous materials, contraband, and/or prohibited items.

3. Internal Controls. These procedures are designed to detect hostile actions within areas, and prevent unauthorized removal of material from areas.

B. Legal Authority.

1. Commanders of military installations have the authority to publish and enforce regulations for safeguarding personnel, facilities, and property. This authority is derived from *The Internal Security Act of 1950* (50 United States Code (U.S.C.) 797), and is implemented by DoDI 5200.8, *Security of DoD Installations and Resources and the DoD Physical Security Review Board* (PSRB), DoD 5200.8-R, *Department of Defense Physical Security Program*, and DLA Instruction 4306, *Physical Security Program* (http://www.dtic.mil/whs/directives/corres/pdf/520008p.pdf / http://www.dtic.mil/whs/directives/corres/pdf/520008r.pdf / https://headquarters.dla.mil/DES/policy/i4306.htm).

2. Jurisdiction. There are four possible types of jurisdiction to be found on U.S. government installations: exclusive, concurrent, partial, and proprietary. Depending upon where an incident occurs on an installation, the jurisdictional status may differ, for an installation may have more than one type of jurisdiction. For those installations or off-installation areas under government control where DLA does not exercise exclusive federal jurisdiction, security forces chiefs must work closely with the PLFA Office of Counsel and local civil authorities to establish protocols for handling civilian violators.

a. Exclusive. The Federal government has retained, or acquired from the state, complete legislative authority, while the state has none except the right to serve state civil or criminal process. HQ Complex and DLA installations in Columbus, OH and Susquehanna, PA are exclusive federal jurisdiction.

b. Concurrent. Both the state and Federal government have complete legislative authority. DLA installations in Richmond, VA, Sharpe and Tracy, CA are concurrent jurisdiction. DLA facilities not mentioned in this paragraph or the paragraph above are tenants on other military installations not under DLA direction or control.

c. Partial. Both the state and Federal government have some legislative authority.

d. Proprietary. The Federal government has acquired some right or title similar to any other private landowner, but the state has retained sole authority to legislate over the area.

3. Continental United States (CONUS): In CONUS, Commanders publish and enforce regulations to protect installation resources in accordance with DoD and DLA policy. In addition, *Title 18 U.S.C. 1382*

prohibits individuals in the United States from entering any military installation for a purpose prohibited by law or lawful regulation or reentering an installation after being ordered not to reenter by any officer in command of the installation.

4. Outside the Continental United States (OCONUS). At OCONUS and its possessions, a Commander's right to exercise this authority comes from United States laws applying in the overseas area and from bilateral and multilateral agreements between the United States and host countries.

C. Establishing and Publishing Local Procedures.

1. Procedures are established to deter unauthorized personnel from entering an installation and to protect installation resources. In establishing procedures, PLFA Commanders/Directors must determine the level of control necessary to prevent property loss and destruction, espionage, terrorism, or sabotage. Requirements and procedures are then published in the installation security plan as appropriate. ***NOTE: The servicing Office of General Counsel must review installation entry procedures for legal sufficiency.***

2. Determining Levels of Control. PLFA Commanders/Directors use the following factors to determine levels of control.

a. The threat to the installation.

b. The protection requirements of assigned resources.

c. Base features that could present significant hazards to public safety.

d. Pilferage problems specific to the installation. (Pilferage is deliberate taking of property through circumvention of human controls and physical protection measures.)

3. Required Minimum Controls. Installation Commanders are required at a minimum to follow policies prescribed in this manual.

4. Installation Commanders/Facility Directors publish installation/facility entry procedures. Ensure procedures allow authorized personnel to enter and leave the base efficiently. Describe and identify the installation boundaries and prohibit anyone from entering without consent of the Installation Commander.

5. Outline any unique entry procedures for contingency operations in an annex to the installation or facility physical security plan.

D. Installation Entry Control Points (Gates).

1. Gates include those used on a routine basis, day-to-day operations, and those staffed only on a specified day or for a specific period of time. Entry control points may be used for vehicles only, pedestrians only, or both. At least one individual at each gate must be armed.

2. Routine Entry Control Points. Pedestrian and vehicle traffic must enter the installation through these entry points. These gates are staffed by security force personnel or trained, armed augmenters (per installation augmentee program).

3. Special-Purpose Entry Control Points. These entry points may be used for pedestrian and vehicle traffic. Personnel trained by the installation security forces, including contractors and owners or users, may open and staff installation special purpose gates. Close and lock these gates during periods of low traffic volume. ***NOTE: The general base populace will not be allowed to use these gates.***

E. Gate Closure Procedures.

The Installation Commander/Director will develop local procedures for gate closure and gate closure devices. Ensure approved procedures, to include alarm and other emergency response procedures to installation gates, are outlined in local directives.

F. Identification Cards.

1. All DLA Activities will establish procedures for the identification and control of personnel and visitors. DoD CAC, dependent, and retiree identification (ID) cards will be used as the principal identity credential to gain access to DLA installations. The use of automated entry control systems at DLA Activities is highly encouraged and recommended. Cards used for these automated systems will be referred to throughout this manual as "key cards." Proposals to automate entry control that impacts upon intent, design, or utilization must be approved by DLA Installation Support, Office of Security and Emergency Services.

a. Facility identification badges will be issued to identify DLA employees within specified facilities and can be programmed to access required security areas. A separate key card or badge may be issued for this purpose. An individual's SSN may not be displayed anywhere on the face, or obverse, of any key cards or Facility identification badges, nor may the SSN be contained in the mag-stripe or memory-chip of such card or badge.

b. PLFA Commanders/Directors may choose to use a key card or badge system to enhance control of movement through any activities under their control.

2. Issuing Authority. No form of DoD identification may be lawfully possessed or used unless it has been approved and issued by an authorized issuing official. The authority to issue identification cards/badges has been delegated to Chiefs, Security and Emergency Services/Chiefs, Security Services, who may also delegate the authority to designated issuing officials.

3. Possession. Each DLA employee is required to possess and carry a form of DoD identification while on duty and on DLA property.

4. Authorized Use.

a. DoD ID cards are intended for official use by the bearers. They are used to identify the bearers as employees or contractors of DoD and to authorize admittance to Federal facilities subject to local controls.

b. DoD ID cards are not intended for use as identification in conducting personal business. However, it is understood that from time to time employees will be required to identify themselves, by name and photograph or by place of employment, for legitimate personal purposes.

c. Any misuse of an ID card , including use for other than official or authorized purposes, repeated loss, or failure to carry it while on duty, may result in retrieval of the card/badge, revocation of the privileges it conveys, or administrative or criminal action. All forms of DoD identification are the property of the U.S. Government and may be retrieved at any time by the issuing official or security authority for just cause.

5. Safeguarding. Blank stocks of ID cards/badges will be maintained under the positive control of the issuing official and, as a minimum, kept in a locked container.

6. Accountability. It is the responsibility of each issuing official to maintain detailed accountability records of all ID cards/badges that have been received or issued. Control ledgers or the automated system for each type of card/badge will show the card number, date of issue, to whom issued, and office of assignment. Upon separation or transfer, an employee must surrender the card/badge to the issuing office and the control ledger or automated system should be annotated accordingly.

7. Inventories. Upon the appointment of an issuing official, an inventory of the blank stocks of controlled ID cards/badges should be conducted and the results reconciled with the control ledger. The issuing official will also conduct an annual inventory of blank stocks of controlled ID cards/badges and reconcile the results with the control ledger. A record of the inventories will be maintained with the control ledger, in accordance with DoD Records Management Program (DoDD 5015.02). Blank cards/badges should be maintained under lock and key at all times, and only authorized individuals should have access.

8. Inspections. The responsible Chief, Security and Emergency Services/Chief, Security Services at activities with designated issuing officials must conduct an annual inspection to insure that the security, issuance, and accounting procedures governing personnel ID cards/badges are in accordance with DoD and DLA Instructions.

9. Other Agency Passes and Credentials. In addition to the DoD CAC, other credentials may be recognized and honored for admission to the facility during hours when such passes and credentials are properly accredited, the bearers are on official business, and local security procedures do not prohibit entry. Future acquisition of physical access control system (PACS) will allow for credential authentication and verification. Included in this category are:

a. All Federal law enforcement credentials;

b. Passes and credentials from other federal government agencies;

c. Passes and identification credentials issued by tenant agencies to their own personnel;

d. Such others as may be designated by the senior officials having jurisdiction of the installation or facility.

10. Disposition of records/files. Documents relating to the request for authorization, issue receipt surrender and accountability records pertaining to identification badges, cards and passes (other than visitor). (Destroy 1 year after obsolete or no longer needed except that individual badges, photographs, or passes will be destroyed upon revocation, cancellation, or expiration and except that credentials relating to personnel barred from facility will be destroyed 5 years after final action to bar facility per N1-361-91-007.)

G. Visitor Identification and Control.

1. Visitors not possessing a DoD issued ID card will need to present a valid US Government ID or driver's license and be processed in accordance with local visitor procedures. Each DLA Activity will develop specific procedures for identification and control of visitors. These procedures will include the following:

a. Positive methods of establishing the authority for admission of visitors, as well as any limitations concerning access.

b. Positive identification of visitors by means of personal recognition, visitor permit, or other identifying credentials. The employee, supervisor, or officer in charge will be contacted to ascertain the validity of the visit.

c. The DLA Form 584, *Visitor Register,* or equivalent will be used to provide a record of the identity of the visitor, time, destination, purpose of visit, duration of visit, and other pertinent control data. Automated systems may be used instead of the DLA Form 584 provided the system records the same data as the DLA Form, at a minimum.

d. Visitor Security Badges. Visitor security badges must be used to identify visitors to DLA Activities. Controls will be established to recover the security badges or render them unusable upon expiration or when no longer needed. Visitor security badges should be numbered serially and should indicate the following:

(1) Bearer's name;

(2) Area or areas to which access is authorized;

(3) Escort requirements, if any;

(4) Time limit for which issued;

(5) Signature of the authenticating official;

(6) Photograph, if desired.

2. The activity's Security Education and Training Program will be tailored to encourage employees to assume a security conscious attitude. DLA employees sponsoring visitors onto the activity are responsible for the visitor's actions while on the activity. Employees will be instructed to consider each unidentified or improperly identified individual as a trespasser. In security areas where access is limited, employees will report the movement of individuals into unauthorized areas.

3. Disposition of records/files. The visitor register shall be destroyed 2 years after last entry per General Records Schedules (GRS) 18, item 17b.

H. Unauthorized Entry.

1. Under *Section 21 of the Internal Security Act of 1950 (50 U.S.C. 797),* any directive issued by the Commander/Director of a military installation or facility, that include parameters for authorized entry to or exit from a military installation, is legally enforceable against all persons, whether or not those persons are subject to the *Uniform Code of Military Justice (UCMJ).* Military personnel who reenter an installation after having been properly ordered not to do so may be apprehended. Civilian violators may

be detained and either escorted off the installation or turned over to proper civilian authorities. Always consult with servicing legal offices when dealing with unauthorized entry situations.

2. Civil Law Enforcement Actions. Civilian violators may be prosecuted under *18 U.S.C. 1382*.

3. Security Forces Actions. If someone enters an installation or facility without authorization, including re-entry following receipt of an order to leave or barment from the installation, security forces must take the following actions.

a. Detain and identify violators;

b. Process a barment order and/or violation notice, order them to leave and, if appropriate, release them to civilian authorities; and

c. Ensure they are escorted off the installation.

I. Random Antiterrorism Measures (RAMs).

RAMs will be identified, addressed in the local AT Plan and implemented in accordance with DoDI 2000.16, "DoD Antiterrorism Standards."

J. Barment Procedures.

1. Under the authority of 50 U.S.C. 797 and DoDD 5200.8, Installation Commanders may deny access to the installation through the use of a barment order. Commanders may not delegate this authority. Barment letters will be coordinated through the servicing Office of Counsel. Documentation supporting barment must be kept for the period of the barment.

2. Barment Orders. Barment orders will be in writing and contain sufficient details to support prosecution by civilian authorities. The barment order must also state a specific, reasonable period of barment. Oral barment orders will be given only when time constraints prevent preparing a written order; they must be immediately followed-up in writing.

a. If practical, barment letters are hand-delivered.

b. If hand delivery is impracticable, barment letters will be sent by certified mail to ensure a record of receipt.

3. Security forces will:

a. Maintain a list of personnel barred from the installation. All lists are For Official Use Only.

b. Use local procedures to update the list.

c. Not release lists to the public, leave them unsecure or place them where unauthorized personnel can view them.

d. Barment lists may be combined with and maintained in the same manner as lists used for tracking and documenting personnel denied on-base driving or other privileges.

K. Vehicle Control

1. Registration.

a. The operation of a privately-owned vehicle (POV) at DLA installations is a conditional privilege granted to eligible personnel by the DLA Installation Commander/Director. These personnel include civilians employed by the installation or its tenants, military personnel assigned to the installation or its tenants, and other designated personnel who are authorized access to the installation frequently. DLA Activities that are tenants on military installations will comply with the host's policies and procedures for the registration of POVs.

b. Comply with the requirements outlined in AR 190–5/OPNAV 11200.5D/AFI 31–218(I)/MCO 5110.1D/DLAR 5720.1, *Motor Vehicle Traffic Supervision* (http://www.army.mil/usapa/epubs/pdf/r190_5.pdf). This regulation establishes policy, responsibilities, and procedures for motor vehicle traffic supervision on both CONUS and OCONUS military installations. This includes but is not limited to the following:

(1) Granting, suspending, or revoking the privilege to operate a POV;

(2) Registration of POVs;

(3) Administration of vehicle registration and driver performance records;

(4) Driver improvement programs;

(5) Police traffic supervision;.

(6) Off–installation traffic activities.

2. Temporary Registration. Vehicles may be registered on a temporary basis for a time period determined locally. Temporary vehicle registration forms will be locally produced and will be displayed on the left front portion of the vehicle's dash.

3. Visitor Passes. Visitors who are authorized entry to the activity may be issued visitor passes in accordance with local procedures.

a. All vehicles of visitors will be recorded on DLA Form 1749, Vehicle Registration Log or in an automated system. The log or automated system will provide the make of the vehicle, license plate number, drivers license number, name of driver, destination, purpose of visit, and time and date of entry and departure.

b. Visitors will be directed to park at specifically designated parking areas. Where visitors are permitted entry to an installation after normal duty hours, local procedures will specify the conditions of entry and other limitations to assure continuous vehicle control.

4. Vehicle Decals. POVs permanently registered for operation on a DLA installation will be identified by using the DD Form 2220, DoD Registered Vehicle (Decal) or locally produced vehicle pass.

a. Decals will be affixed as directed locally. Locations such as the front window, where permitted by state motor vehicle laws, or on a locally obtained metal or plastic plate that is affixed to the vehicle's front license plate (holder) may be used.

b. The Installation Chief, Security and Emergency Services/Chief, Security Services will procure, control, and issue the DD Form 2220 as an accountable form.

c. Vehicle decals will be issued at no cost to the registrants.

d. Unless security requirements dictate otherwise, valid DoD decals issued by other DLA installations, DoD agencies, or the Military Services may be honored for visitors to all DLA installations.

e. Expiration tabs will consist of bold block numbers; e.g., 6-81 (month and year), using time-colored background with black numbers. Tabs should be no larger than 3 1/4-inches wide by 1 1/2-inches long.

f. Additional controls may be established locally. These may include but are not limited to the following:

(1) Requirement for an expiration tab;

(2) Random checks to determine compliance;

(3) Issuance of supplemental decals to identify vehicles registered to senior military personnel and/or retired military personnel.

g. The registration will remain valid during the registrant's employment or assignment to the installation unless it is declared invalid for any reason, such as a revocation of driving privileges.

5. Termination of Registration. Issued decals remain U.S. Government property and will be removed by the registrant. The decal pieces will be returned to the vehicle registration office when:

a. The registrant sells or otherwise disposes of the vehicle.

b. The registrant's installation driving privileges are suspended or revoked.

6. Vehicle Parking Control. For increased force protection conditions, each installation will have a parking plan that describes measures put in place to ensure parking areas for POVs are in accordance with AT/FP standoff requirements. Parking areas will be lighted when used during the hours of darkness. The method of parking should be clearly marked and strictly enforced.

7. Disposition of records/files. Documents and records relating to permanent motor vehicle registration of private vehicles to include commercial vehicles shall be destroyed upon normal expiration or supersession of registration or 3 years after the revocation of registration per N1-361-91-1.

L. Photography

1. It is unlawful to make any photographs, sketches, picture, drawings, maps, or geographical representations of areas designated as classified or restricted. Each DLA Installation and stand-alone facility will publish policies and procedures to supplement these instructions that are specific to their location; DLA entities that are tenants will coordinate local policy with their host. Written procedures will be established and coordinated, at a minimum, with supporting legal and strategic communications offices.

2. Local policies and procedures must address the following areas:

a. Use of photographic and recording equipment by all personnel, including but not limited to DoD civilians, military members, family members, and contractors at non sensitive areas/social events.

b. Approval process for use of photographic/recording equipment and procedures for when and where equipment may be used (i.e. graduations, weddings, OIG inspections, surveys, and/or additional mission requirements).

c. Procedures for securing unapproved photographic/recording equipment from individuals until the content or equipment has been appropriately adjudicated.

d. Consideration of potential administrative and/or disciplinary actions for policy violators.

3. Members of civilian or Department of Defense (DoD) media are prohibited from bringing photographic/recording equipment to DLA locations unless prior authorization is granted by DLA Strategic Communications. Members of the media must be accompanied by a DLA Strategic Communications representative during photo or video shoots. Additionally, the local Chief of Security and Emergency Services shall be notified in advance of any media events to ensure guidance is provided concerning classified or restricted areas. NOTE: When members of the media make unannounced visits to a DLA installation or facility, they will not be allowed access without escort by DLA Strategic Communications.

CHAPTER 3: PERIMETER CONTROL

A. General.

A physical barrier defines the boundary of a security area and limits access thereto. It also:

1. Creates a physical and psychological deterrent to entry.

2. Delays intrusion into the area, thus making the detection and apprehension of intruders by security personnel more likely.

3. Facilitates effective and economical utilization of security force personnel.

4. Channels the flow of personnel and vehicles through designated portals in a way that permits effective and efficient identification and control.

B. Planning Considerations.

Physical barriers will delay but will not stop a determined intruder. Therefore, to be fully effective, barriers must be augmented by security force personnel. In determining the type of structural barrier required, the following factors will apply:

1. All DLA installations/facilities will have escorted and unescorted access control procedures. Visitors must access the installation/facility via authorized entry control points and must possess valid credentials.

2. Physical barriers will be established around all secure areas and around DLA installation perimeters.

3. Planning must take into account issues such as: safety, fire protection, functional and operational issues, energy conservation, and handicapped access.

C. Fencing.

Fencing used for installation perimeters and for the protection of permanent security areas must meet the requirements set forth by the U.S. Army Corps of Engineers and be constructed and configured as set forth below:

1. Fence Fabric. Installations must use woven 9-gauge (.1483 inches or 3.7 mm), steel-wire, chain-link fabric with 2-inch (5.1 cm) square mesh. Steel-wire fabric must have a steel core that measures 9 gauge, not including the coating. Use non-reflective paint for fences to reduce glare that could affect remote camera and visual assessment. Coated steel wire purchased or installed before 1 January 1980 meets the 9-gauge steel core requirement as long as the core wire is at least 11 gauge (.1205 inches or 3.1 mm).

2. Fence Height. The above ground height of the mesh fabric must measure 7 feet (approximately 2.13 m).

3. Fence Mounting. Fences are mounted as follows:

a. Mount fence fabrics on metal posts of appropriate height set in concrete with additional bracing at corners and gate openings, as necessary**.** Use reinforced concrete posts if metal posts are not available.

b. Put posts, bracing, and other structural members on the inside (site side) of the fence fabric.

c. Secure the fence fabric to fence posts, rails, or other anchoring material with fasteners of tensile strength at least equal to that of the fence fabric. Firmly secure fence fabric to tension wires with 12-gauge galvanized tie wire incorporating at least a 540-degree tightened loop.

4. Fence Topping. Outriggers. Steel outriggers will be installed to conform with RR-F-191/4 with their overhang facing outward (away from the protected site) each having three strands of barbed wire, at intervals along the top of the fence line (see figure 1 below), except where the fence must be mounted directly on the property line (instead of at least 18 inches (457.2 mm) back), in which case outriggers can be modified (with exception approval) to be vertical or angle into the site. As a minimum, the outriggers will provide an additional 12 inches (304.8 mm) to the fence height. The top guard fencing adjoining gates may range from a vertical height of 18 inches (457.2 mm) to the normal 45-degree outward protection, but only for sufficient distance along the fence line to open the gates adequately. Outriggers will be permanently affixed to the fence posts with screws or by spot welding.

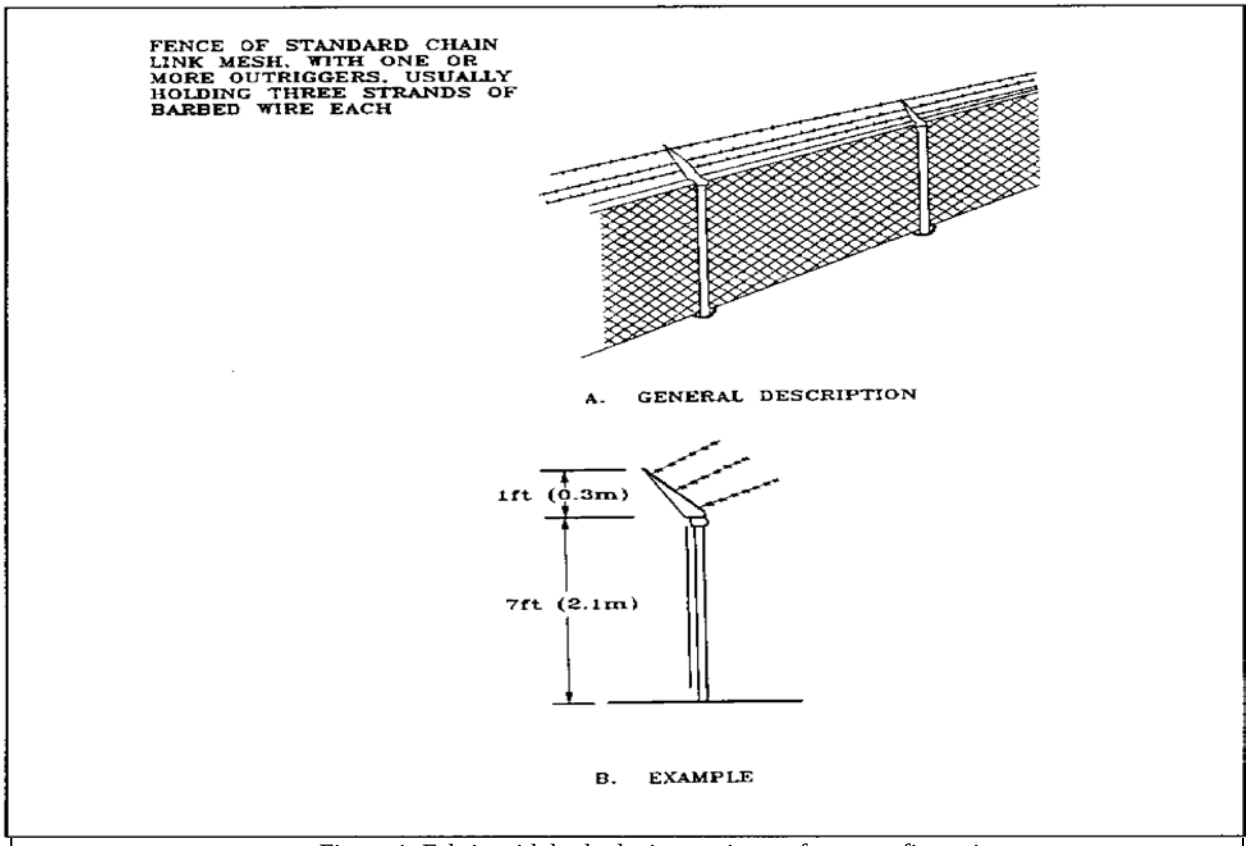

Figure 1. Fabric with barbed wire outriggers fence configuration

5. Anchoring and Stabilizing Fences. Extend the bottom of the fence fabric to within 2 inches (5 cm) of firm ground and anchor it to prevent intruders from lifting the fabric and creating an opening more than

5 inches (12.5 cm) in height. To do this, use horizontal bottom rails, concrete curbs or sills, sheet piling, piping, or other inexpensive materials.

a. Stabilize surfaces in areas where loose sand, shifting soils, or surface waters cause erosion that could allow an intruder to penetrate the perimeter security system.

b. Where you can't stabilize the surface, provide concrete curbs, sills, or other similar types of anchoring devices and extend them below ground level.

c. During installation, stabilize fencing that also serves as a sensor system platform to meet sensor-sighting requirements.

6. New construction or modifications of existing fencing will be in accordance with these requirements. Existing fencing that does not meet the minimum height requirements outlined above will not be increased to the specified height provided the existing fence is in good repair and has an overall height to include barbed wire top guard of 7-feet.

D. Barrier Openings.

1. The barrier will have a minimum number of vehicular and pedestrian gates consistent with operational requirements. Such gates will be structurally comparable and provide equal or greater resistance to penetration as the adjacent fence.

a. The gate fabric or support must reach to within 5 inches of paved surfaces and to within 2 inches of other surfaces. It must prevent someone from lifting the fabric to create an opening more than 5 inches high. The maximum allowable distance between the gateposts and gate is 5 inches when the gate is closed.

b. Gates must be closed and locked when not in use. Gates are considered locked when they are equipped with an electric opening or closing device that, when closed, prevents the gate from being opened by hand.

c. Use a type II or III secondary padlock on manually operated gates that do not have an electric lock. Secure keys at the entry control point.

2. Drainage structures and water passages penetrating the barrier will be barred to form obstacles to unauthorized entry and be of equivalent strength as the fence itself. Openings to drainage structures having a cross-sectional area greater than 96 square inches and a smallest height or width dimension greater than 6-inches, will be protected by securely fastened, welded-bar grills.

3. Gate houses at DLA Installation entry points will be constructed, in compliance with UFC 4-022-01, to facilitate traffic control and visibility for security force members guarding the installation. They will be permanently constructed with the safety of the installation entry controller in mind. As a rule, they will be located in the center of the roadway and will include:

a. Entrances to both entry and exit roadways;

b. Telephone lines to the police force desk;

c. Duress alarms that annunciate at the security operations center;

d. Radio communication;

e. Entry and exit barriers and vehicle deflectors (to prevent runaway vehicles from hitting the gate house); use UFC 4-022-02 for selection and application of vehicle barriers;

f. Lighting for nighttime operations;

g. Infrastructure to support future PACS implementation.

E. Walls and Other Structural Barriers.

1. Where walls serve as barriers, they will be constructed and arranged to provide uniform protection equivalent to that provided by the chain link fencing specified above.

2. Where a fence adjoins a perimeter wall, it will extend to within 2-inches of the building wall.

3. Miscellaneous openings requiring bar or grill protection include:

a. Openings less than 18-feet above uncontrolled ground, roofs, or ledges.

b. All openings having an area of 96 square inches or larger, and a minimum height or width dimension of 6-inches or greater.

F. Barrier Inspection.

1. The Chief, Security and Emergency Services/Chief, Security Services will ensure that all security perimeter barriers are inspected a minimum of once per shift daily. Additional barrier inspection policy must be a part of the barrier plan included in the Installation /Facility AT Plan. Deficiencies or weaknesses will be reported to the Facility Engineer.

2. A written entry of the inspection to include the name of the individual conducting the inspection, time, and date will be made in the Security Forces blotter. When deficiencies or weaknesses are reported, the deficient item(s), the reporting and receiving official, time, and date will be recorded in the blotter.

3. The Chief, Security and Emergency Services/Chief, Security Services will ensure that barrier deficiencies and weaknesses found during daily inspections are corrected as soon as possible.

G. Clear Zones and Standoff Distances.

1. An unobstructed area or clear zone will be maintained on both sides of the perimeter barrier to provide an unobstructed view of the barrier and the adjacent ground. As a minimum, the clear zone shall extend 20 feet on the outside and 30 feet on the inside of the perimeter barrier.

2. When it is not possible to have adequate clear zones or standoff distances because of property lines or natural or man-made features, an increase in protection measures or other compensatory measures may be necessary.

3. Vegetation within clear zones will be maintained at a height not to exceed 8-inches.

4. When the perimeter barrier encloses a large area, an interior, all-weather road will be provided for use of security patrol vehicles if:

a. Perimeter barriers cannot be adequately patrolled by using exterior public highways that parallel it.

b. The size of the area precludes the use of normal means of surveillance.

CHAPTER 4: LOSS/CRIME PREVENTION

A. Responsibilities.

1. DLA PLFA Commanders/Directors will implement loss prevention procedures that provide for the protection of Government property from loss, theft, and damage. Elements will include: (1) Prevention of losses through physical protection measures and education of employees; (2) Investigations of losses to identify criminal activity and recover material; and (3) Collection of loss data for subsequent investigations and analyses.

2. DLA PLFA Commanders/Directors will establish a positive system of control over cargo, material, and packages moving in and out of their respective activities.

3. DLAR 4145.11, *Safeguarding of DLA Sensitive Inventory Items, Controlled Substances, and Pilferable Items of Supply* (http://www.dla.mil/dlaps/dlar/r4145.11.pdf), prescribes security policy, responsibilities, and procedures for the receipt, storage, shipment, and safeguarding of DLA sensitive inventory items, controlled substances, and pilferable items of supply. A description of these items is provided below.

a. Selected sensitive inventory items – those items security coded "R" or "Q" in the Defense Integrated Data System (DIDS) that are controlled substances, drug abuse items, or precious metals (DoD 4100.39-M, Volume 10, Chapter 4, Table 61).

b. Coded "R" Items – Precious metals, drugs, or other controlled substances designated as a schedule I or II item, in accordance with Public Law 91-513. Other selected sensitive items requiring storage in an exclusion area, i.e., vault or safe, are included.

c. Coded "Q" Items – Drugs or other controlled substances designated as a Schedule III, IV, or V items, in accordance with Public Law 91-513. Tobacco products and other sensitive items, requiring limited access area security, are included.

d. Pilferage Codes – Pilferable items other than sensitive inventory items and controlled substances, having a unit of use weight of 25 pounds or less, cube of 1.0, unit price of $5.00 or more, and a history of unexplained losses or known theft. DoD 4500.32-R. Volume I, specifically includes alcohol in this category. Also specifically included in this category are "Narcotics Paraphernalia."

e. Narcotics Paraphernalia – Hypodermic needles and syringes and related drugs (e.g., lactose, mannitol) used in the illegal administration of heroin, other hard narcotics or dangerous drugs.

f. Precious Metals – Refined silver, gold, platinum, palladium, iridium, rhodium, osmium, and ruthenium, in bar, ingot, granulation, sponge, or wire form. (This does not include items containing precious metals unless so designated by the PLFA Commander/Director.)

g. Controlled Substance – A drug, other substance, or immediate precursor included in Schedule I, II, III, IV, or V of Part B, Title II, Public Law 91-513, and coded "R" or "Q."

4. The Chief, Security and Emergency Services/Chief, Security Services will:

a. Ensure all employees receive initial and annual training in loss prevention.

b. Ensure all sensitive, controlled, and DLA owned/managed assets, cargo, and material are adequately protected and that proper controls are in place and enforced to prevent losses.

c. Collect loss data. This information may be received from several sources but at a minimum will include: (1) Reports of suspected theft or damage; (2) DD Forms 200, *Financial Liability Investigation of Property Lost*.

d. Review loss reports to determine necessity of immediate investigation by DLA Office of Inspector General. (All reports of suspected criminal activity must be investigated immediately upon notification of the incident).

e. Analyze loss data to identify trends or suspicious activity. All analyses should be conducted at the lowest level possible, (i.e., PLFA, Directorate, etc.). Analyses may also be conducted at the Region or DLA level to identify broader trends. An effective analysis of losses should include but not be limited to the following concerns: (1) Losses of similar items; (2) Several losses occurring in a specific location or warehouse; (3) Losses occurring during a specific time of year or time of day; and (4) Losses occurring under similar circumstances.

f. Use analyses to investigate suspicious persons or activities or to improve protection for specific items.

g. Use loss data to provide justification for security improvements/enhancements.

B. Methods of Obtaining Data.

The Chief, Security and Emergency Services/Chief, Security Services will ensure that all personnel are regularly instructed in reporting requirements for thefts or suspicious losses of material. All losses of controlled items are to be immediately reported to the Chief, Security and Emergency Services/Chief, Security Services and/or DLA Office of Inspector General.

C. Preventing Pilferage.

Pilferage is the deliberate taking of property through circumvention of human controls and physical protection methods. Like the terms “steal”, “take”, “theft”, and “larceny”, it implies the taking without authorization of any quantity of material or any item of value. It is every employee’s responsibility to prevent and report pilferage. Pilferage can be reduced and controlled through the use of logical and well-planned protection techniques, which will be used particularly for sensitive items such as small arms, ammunition, computers, and bulk explosives. Commanders/Directors, and Managers must establish programs to ensure accountability and responsibility for resources.

D. Internal Physical Security Measures.

1. Doors.

a. A door is a vulnerable point of the security of any building.

(1) A door must be installed so the hinges are on the inside to preclude removal of the screws or the use of chisels or cutting devices.

(2) Pins in exterior hinges must be welded, flanged, or otherwise secured, or hinge dowels must be used to preclude the door's removal.

(3) The door must be metal or solid wood. Remember that locks, doors, doorframes, and accessory builder's hardware are inseparable when evaluating barrier value.

(4) Do not put a sturdy lock on a weak door. The best door is of little value if there are exposed removable hinge pins, breakable vision panels, or other weaknesses that would allow entry.

(5) Transoms must be sealed permanently or locked from the inside with a sturdy sliding bolt lock or other similar device or equipped with bars or grills.

b. Overhead roll doors not controlled or locked by electric power must be protected by slide bolts on the bottom bar.

c. Chain link doors must be provided with an iron keeper and pin for securing the hand chain.

d. The shaft on a crank operated door must be secured. A solid overhead, swinging, sliding, or accordion type garage door must be secured with a cylinder lock or padlock. Also, a metal slide bar, bolt, or crossbar must be provided on the inside.

e. Metal grill-type doors must have a secured metal guide track at the top and bottom and be secured with a cylinder lock or padlock.

2. Windows. Windows are another vulnerable point for gaining illegal access to a building.

a. Windows must be secured on the inside using a lock, locking bolt, slide bar, or crossbar with a padlock.

b. The window frame must be securely fastened to the building so that it cannot be pried loose.

c. As with glass panels in a door, window glass can be broken or cut so the intruder can reach inside and release the lock.

d. Bars and steel grills can be used to protect a window. They must be at least one half inch in diameter, round, and spaced apart six inches on center. Prior to installing bars or steel grills, security personnel shall consult with the installation fire prevention office to determine if current codes prohibit this measure.

e. If a grill is used, the material must be number nine gauge two-inch square mesh.

f. Outside hinges on a window must have non-removable pins. The hinge pins must be welded, flanged, or otherwise secured so they cannot be removed. Bars and grills must be securely fastened to the window frame so they cannot be pried loose.

3. Manholes, Grates, and Storm Drains. Many facilities have manholes and tunnels providing service entrance into buildings. Other manholes may provide entrance to tunnels containing pipes for heat, gas, water, and telephone. If a tunnel penetrates the interior of a building, the manhole cover must be secured.

a. A chain or padlock can be used to secure a manhole.

b. Steel grates and doors flush with the ground level may provide convenient access. These openings may be designed into the facility as they may provide light and ventilation to the basement levels. If the frame is properly secured, the grates or doors can be welded into place or they can be secured with a chain and padlock.

c. Sewers or storm drains that might provide an entrance must be secured.

4. Roof Openings. Openings in elevators, penthouses, hatchways, or doors to the roof are often overlooked because of infrequent use. Access to a building's roof can allow ingress to the building and access to air intakes and building Heating, Ventilating, and Air-Conditioning (HVAC) equipment (e.g., self-contained HVAC units, laboratory or bathroom exhausts) located on the roof. From a physical security perspective, roofs are like other entrances to the building and must be secured appropriately. Roofs with HVAC equipment must be treated like mechanical areas. Fencing or other barriers must restrict access from adjacent roofs. Access to roofs must be strictly controlled through keyed locks, keycards, or similar measures. Skylights are another source of entry from the roof. These openings can be protected like windows - with bars or mesh. Such protection should be installed inside the openings to make it more difficult to remove.

5. Mechanical Areas.

a. Prevent Public Access to Mechanical Areas. Mechanical areas may exist at one or more locations within a building. Some mechanical areas have access from the perimeter other mechanical areas may only have access from the interior of a facility. These areas provide access to centralized mechanical systems (HVAC, elevator, water, etc.) including filters, air handling units, and exhaust systems. Such equipment is susceptible to tampering and may subsequently be used in a chemical, biological, or radiological (CBR) attack. Keyed locks, keycards, or similar security measures should strictly control access to mechanical areas. Additional controls for access to keys, keycards, and key codes should be strictly maintained.

b. Restrict Access to Building Operation Systems by Outside Maintenance Personnel. To deter tampering by outside maintenance personnel, a building staff member must escort these individuals throughout their service visit and must visually inspect their work before final acceptance of the service. Alternatively, building owners and managers can ensure the reliability of pre-screened service personnel from a trusted contractor.

6. Facility HVAC Systems. Ventilation shafts, vents, or ducts, and openings in the building to accommodate ventilating fans or the air conditioning system can be used to introduce CBR agents into a facility. Decisions concerning protective measures should be implemented based on the perceived risk associated with the facility and its tenants, engineering and architectural feasibility, and cost. Specific physical security measures to consider for the protection of the building HVAC system are cited below.

a. Prevent Access to Outdoor Air Intakes. One of the most important steps in protecting a building's indoor environment is the security of the outdoor air intakes. Outdoor air enters the building through these intakes and is distributed throughout the building by the HVAC system. Introducing CBR agents into the outdoor air intakes allows a terrorist to use the HVAC system as a means of dispersing the agent throughout a building. Publicly accessible outdoor air intakes located at or below ground level are at most risk – due partly to their accessibility (which also makes visual or audible identification easier) and partly because most CBR agent releases near a building will be close to the ground and may remain there. Securing the outdoor air intakes is a critical line of defense in limiting an external CBR attack on a building.

(1) Relocate Outdoor Air Intake Vents. Relocating accessible air intakes to a publicly inaccessible location is preferable. Ideally, the intake should be located on a secure roof or high sidewall. The lowest edge of the outdoor air intakes should be placed at the highest feasible level above the ground or above any nearby accessible level (i.e., adjacent retaining walls, loading docks, and handrail). These measures are also beneficial in limiting the inadvertent introduction of other types of contaminants, such as landscaping chemicals, into the building.

(2) Extend Outdoor Air Intakes. If relocation of outdoor air intakes is not feasible, intake extensions can be constructed without creating adverse effects on HVAC performance. Depending upon budget, time, or the perceived threat, the intake extensions may be temporary or constructed in a permanent, architecturally compatible design. The goal is to minimize public accessibility. In general, this means the higher the extension, the better – as long as other design constraints (excessive pressure loss, dynamic and static loads on structure) are appropriately considered. An extension height of 12 feet (3.7 m) will place the intake out of reach of individuals without some assistance. Also, the entrance to the intake should be covered with a sloped metal mesh to reduce the threat of objects being tossed into the intake. A minimum slope of 45 degrees is generally adequate. Extension height should be increased where existing platforms or building features (i.e., loading docks, retaining walls) might provide access to the outdoor air intakes.

(3) Establish A Security Zone Around Outdoor Air Intakes. Physically inaccessible outdoor air intakes are the preferred protection strategy. When outdoor air intakes are publicly accessible and relocation or physical extensions are not viable options, perimeter barriers that prevent public access to outdoor air intake areas may be an effective alternative. Iron fencing or similar see-through barriers that will not obscure visual detection of terrorist activities or a deposited CBR source are preferred. The restricted area should also include an open buffer zone between the public areas and the intake louvers. Thus, individuals attempting to enter these protective areas will be more conspicuous to security personnel and the public. Monitoring the buffer zone by physical security, closed circuit television (CCTV), security lighting, or intrusion detection sensors will enhance this protective approach.

b. Secure Return Air Grilles. Similar to the outdoor-air intake, HVAC return-air grilles that are publicly accessible and not easily observed by security may be vulnerable to targeting for CBR contaminants. Public access facilities may be the most vulnerable to this type of CBR attack. A building-security assessment can help determine, which, if any, protective measures to employ to secure return-air grilles. Take caution that a selected measure does not adversely affect the performance of the building HVAC system. Some return-air grille protective measures include:

(1) Relocating return-air grilles to inaccessible, yet observable locations;

(2) Increasing security presence (human or CCTV) near vulnerable return-air grilles;

(3) Directing public access away from return-air grilles; and

(4) Removing furniture and visual obstructions from areas near return-air grilles.

c. Implement Security Measures, such as Guards, Alarms, and Cameras To Protect Air Intakes or Other Vulnerable Areas. Difficult to reach out-door air intakes and mechanical rooms alone may not stop a sufficiently determined person. Security personnel, barriers that deter loitering, intrusion detection sensors, and observation cameras can further increase protection by quickly alerting personnel to security breaches near the outdoor air intakes or other vulnerable locations.

d. Restrict Access To Building Information. Information on building operations – including mechanical, electrical, vertical transport, fire and life safety, security system plans and schematics, and emergency operations procedures – should be strictly controlled.

7. Fire Escapes and Building Walls.

a. Normally, outside fire escapes do not provide an entrance directly into the building. However, they can provide easy access to the roof or openings high above the ground level. Windows or other openings off the fire escape should be capable of being opened only from the inside. The exterior fire escape should not extend all the way to the ground.

b. Walls are not normally considered possible points of entry because of their usual solid construction. However, they cannot be disregarded because intruders may be able to break through them to gain entrance. Reinforcement at critical points may be necessary to deter forced entry.

8. Cargo and Material Control.

a. DLA PLFA Commanders/Directors will establish written procedures to control the movement of material and cargo entering, circulating within, and departing DLA Activities. Such procedures will provide adequate security controls to reduce the opportunity for theft or diversion of Government property with minimum delay to traffic flow and installation mission accomplishment.

b. Truck Control. Locally developed truck control procedures will, at a minimum, meet the following requirements outlined below:

(1) When feasible, a single gate will be used for the truck traffic.

(2) Sponsors will ensure truck operators are pre-announced prior to their arrival at all installation entry control points.

(3) Incoming trucks will be inspected by security force personnel for unauthorized personnel and the correct number of applied seals as indicated on applicable shipping documents.

(4) Operators will be informed that firearms, illicit drugs, and other contraband are not authorized on the installation. Local procedures will be established which provide guidance to security force personnel concerning firearms, pet, and rider control.

(5) After registration and inspection, an intradepot seal will be affixed to the truck and the driver will proceed to the receiving or shipping areas via an authorized route.

(6) Out-bound trucks with over-the-road seals will be inspected to ensure that affixed seal numbers agree with shipping documentation. Partially loaded trucks departing the activity will be inspected by comparing affixed intradepot seals with shipping documentation. Empty trucks will be visually inspected prior to departure. All intradepot seals will be removed prior to the truck's departure. Trucks will not proceed until discrepancies have been resolved.

(7) Local procedures will also include instructions for hours during which trucks may enter and depart the activity, controls during non-duty hours, weekends, and holidays, authorized parking area(s), and provisions for overnight parking and security of trucks and trailers.

(8) DLA Form 1617, *Cargo Movement and Seal Record*, shall be executed in triplicate for each truck (van and flatbed) entering a DLA Activity. The transportation office will provide the DLA Form 1617 to all truckers. The original and duplicate will be given to the driver who must present it to each shipping and receiving point he visits. The triplicate form will be retained by security personnel manning the installation entry control point. An authorized individual at each truck stopping point will sign the form noting the times of arrival and departure of the truck. Upon departing the installation, the driver will be required to surrender the original and duplicate copy of the form. At the end of each guard shift, an inventory will be conducted to ensure that all originals and duplicates issued during that shift have been returned. At this time, the relief security supervisor and the relief guard at the access control point will be advised of any documentation discrepancies and the number of trucks remaining in the area. The file of triplicates retained by the security personnel serves as the truck register for a tour of duty. Later, the original and duplicate will be reunited with the triplicate and will serve as a history of each transaction. After the comparison of all the copies has been satisfactorily made, the original and triplicate will be filed by the activity's Chief, Security and Emergency Services/Chief, Security Services and the duplicate will be given to the Director.

(9) DLA Form 1749, *Vehicle Registration Log*, or an automated system containing the same information, will be completed by security force personnel manning the installation gates. The log maintained by police gate guards will include as a minimum the vehicle tag number, operator's name and signature, destination, date and time of departure and return to the installation.

c. The following categories of trucks are normally exempted from the provisions of this section; however, this exemption does not prohibit the Commander/Director from establishing controls for such trucks.

(1) Local activity trucks when performing normal functions on the activity. (NOTE: This exemption does not include those local activity trucks engaged in pickup and delivery of depot mission stock between the activity and off-post locations such as airports, freight terminals, etc.)

(2) Emergency vehicles when responding to an emergency.

(3) Flatbed trucks are exempt from truck control requirements. However, instead of sealing, a Dray Ticket will be used. If these type vehicles are required to make deliveries between depots, the vehicle's odometer reading will be recorded on the Dray Ticket as the vehicle exits and enters the activity.

d. DLA Activities that are tenants on military installations will establish and operate, to the fullest extent possible, a truck control system comparable to that outlined in this section that does not conflict with host installation regulations or operating procedures.

e. Railroad Car Control. Locally developed procedures for the control of railroad cars will, at a minimum, include the following requirements:

(1) The movement of railroad cars in and out of DLA Activities will be supervised by DLA personnel and observed by security forces.

(2) All railroad entrances will be secured when not in use. Security forces will provide access control during passage of railroad cars.

(3) Keys to railroad gates will be controlled by security forces.

(4) Security personnel will inspect the cargo seals on all incoming and outgoing railroad cars at the entry control point. Empty railroad cars will be inspected for contraband, hazardous items, and unauthorized personnel. Local procedures will be established which provide guidance to security force personnel when discrepancies are found during this inspection. Whenever railroad cars are staged at warehouse locations, partially loaded cars will be sealed at the close of loading operations and will be checked by security patrols.

(5) Railroad seals will be affixed and verified in the same manner as that prescribed for truck control.

9. Package Control. Property controls will not be limited to packages carried openly, but also include controls of articles of clothing, handbags, or anything else of a similar nature that may be used to conceal property or material.

10. Searches and Inspections. Each activity's search policy will be formally developed using guidance contained in the DLA Instruction 4302, *Force Protection and Security Operations*.

E. Seals.

1. The purpose of a seal is to detect whether the integrity of a storage facility, vehicle, rail shipment, or container has been compromised. An integrity seal is not a lock; however, some seals may have a secondary function as a locking device.

2. Seal construction specification will include:

a. Durability - Seals will be strong enough to prevent accidental breakage during normal use. Use of metal seals is encouraged.

b. Design - Seals will be sufficiently complex to make unauthorized manufacture of a seal difficult.

c. Tamper Proof - Seals will readily provide visible evidence of tampering and be constructed in a way that makes simulated locking difficult once the seal has been broken.

d. Individually Identifiable - Seals will have embossed serial numbers and owner identification.

3. Seals will be requisitioned and issued by a designated, centralized office within the DLA Activity

4. Intradepot seals should be a different color than over-the-road seals and should have a separate serial number sequence. This allows security personnel to differentiate between internal/external seals.

5. Accountability and Application. The purpose of a numbered seal is defeated if strict accountability and controlled application are not maintained. Accountability begins with the manufacturer and is terminated when the seal is destroyed. Locally developed procedures will, at a minimum, include the following requirements:

a. Seals not issued for immediate use will be stored in a locked container. Access to stored seals will be restricted to authorized personnel.

b. Seal Custodians and personnel authorized to apply and remove seals will be appointed in writing. These appointments will be kept to a minimum commensurate with operational requirements.

c. The office that requisitions and receives seals for the activity will maintain a seal log (hard copy and/or electronically). All seals will be logged by serial number upon receipt. Log entries pertaining to the issue of seals to subordinate custodians will include the date of issue, the name of the recipient, the quantity issued, and the serial numbers issued. The recipient will sign a receipt indicating the quantity and serial numbers received.

d. Each subordinate custodian will also maintain a seal log (hard copy and/or electronically). Each seal will be individually logged by serial number upon receipt. Log entries pertaining to the issue of seals for immediate use will include the date and the applied seal serial number, identification of item to which applied, and the name of the person applying the seal. For outbound loaded trucks, rail cars, and container shipments, the appropriate truck, rail cars, or container number and Government Bill of Lading (GBL) number should be noted in the log.

e. The serial numbers of applied seals will also be recorded on the DLA Form 1617 and the GBL when over-the-road seals are applied by the Transportation Office.

f. Trucks will be sealed as soon as final loading is completed. Rollup type doors will be sealed by an authorized individual at the dock before the truck is moved. In case of swingout doors, the driver will pull the unit out upon completion of loading so that seals can be applied.

g. Side doors and other openings providing access to cargo compartments will also be sealed.

h. Procedures will be established to examine seals on cargo doors at each intradepot stop. Upon exit from the activity, gate guards will conduct a check to ensure that over-the-road truck and rail car seals correspond with the seal numbers annotated on the DLA Form 1617.

i. Intradepot seals applied to record the integrity of shipments on the activity will be removed prior to the vehicle departing the activity. Over-the-road seals placed on vehicles by the Transportation Office and recorded on the GBL and DLA Form 1617 will not be removed by security force personnel. Intradepot seals removed must be deformed sufficiently so that they cannot be used to simulate a good seal.

6. Whenever a seal is suspected of having been compromised, the following information will be noted on the DLA Form 1617:

a. Date and time of discovery.

b. Name and organization of person making the discovery.

c. Circumstances.

d. Serial numbers of new seals applied.

e. Name and organization of person applying the new seals.

f. Name and organization of witnesses.

7. Trucks with suspect seals will be held until it is determined that there are no discrepancies in the shipment. When discrepancies are discovered, these will be thoroughly investigated and results of the investigation documented. Preliminary investigations will be completed by the on duty Police Officer and transportation personnel. If further investigation is needed, it will be conducted by the DLA Office of Inspector General.

8. The above procedures will also apply to seals on railroad cars.

CHAPTER 5: PROTECTIVE LIGHTING

A. General.

Requirements for protective lighting will depend upon the situation and areas to be protected. Therefore, specific requirements for types of lighting will be determined locally. Each situation requires careful study to provide the best visibility that is practical for security duties such as recognition of personnel and identification at gates, inspection of vehicles, prevention of unauthorized entry, detection of intruders, and investigation of unusual or suspicious circumstances. Where such lighting provisions are impractical, additional security posts, patrols or other security measures will be employed. Facility Engineers at DLA Activities will assist in designing the lighting system.

B. Planning Considerations.

1. In planning a protective lighting system, the Chief, Security and Emergency Services/Chief Security Services and the Facility Engineer must be aware of the following considerations:

a. Cleaning and replacement of lamps and luminaries, particularly with respect to acquisition costs and equipment availability.

b. The advisability of including manual and photoelectric controls.

c. The effects of local weather conditions on various types of lamps and luminaries.

d. Fluctuating or erratic voltages in the primary power source.

e. The requirement for grounding of fixtures and the use of a common ground on the entire line.

f. Energy conservation (cost versus security). Contact the local environmental office for additional information and advice.

2. Fixture characteristics, selection, and other related technical data are considerations for which the Facility Engineer is primarily responsible. Security personnel should assist, however, by supplying information concerning desired operational requirements, flexibility required in lighting use, and like data.

3. Design. Interior and exterior lighting systems, including fixtures, lamps, and associated primary and backup power and control components and wiring must be carefully designed. Engineering and security forces personnel must coordinate closely on each phase of lighting projects to ensure all requirements such as illumination levels, uniformity, color rendering, and energy conservation are adequately identified and addressed.

4. All lighting projects must be coordinated with the Safety Office.

5. Plan and design lighting systems, switches, power lines, and supporting equipment carefully. Each must be placed so that an intruder cannot defeat the lights by simply turning them off or cutting a power supply.

6. For additional information refer to Unified Facilities Guide Specifications (UFGS) 26 55 53.00 40, "Security Lighting."

C. Lighting Requirements and Specifications.

1. Types of Lighting Systems. Four basic lighting systems may be used depending on the location and type of resource to be protected. Often a combination of two or more types is necessary. Before determining the type of lighting system to be installed, analyze background shading and coloring differences. Dark backgrounds require more illumination than light colored surfaces. Physical security personnel should influence construction plans to achieve the most cost-effective shading for enhanced illumination.

a. Boundary Lighting. Constant boundary lighting is required when the resource to be protected justifies boundary fencing. Boundary lighting covers the area outside the fence or physical barrier so that it will not only expose anyone approaching the area, but will also limit or restrict the vision of anyone outside the area trying to look in.

b. Area Lighting. Area lighting is designed to illuminate the area within the fence or boundary or illuminate the exterior of a building to enhance visibility. Lighting for limited access areas such as Restricted and Controlled Areas must remain on at all times during hours of darkness or low visibility.

c. Entry Point Lighting. Constant installation and facility entry point lighting is required. It must be especially well lit at an entry point where an entry controller may be required to see and recognize persons at some distance.

d. Special Purpose Lighting. Special purpose lighting may include portable lights, spotlights, searchlights, or ball park lights.

2. Critical structures and areas will be the first considerations in designing protective fencing and lighting. Power, heat, water, communications, explosive materials, and Restricted and Controlled Areas need special attention.

3. Entry control points will be provided with constant, adequate illumination for recognition and identification of personnel. All vehicle entrances will have adequate lighting units so positioned as to facilitate complete inspection of vehicles, their contents, and passengers. Gate houses will have a low level of interior illumination to enable security personnel to see adequately, increase their night vision adaptability, and avoid making them a target.

D. Wiring.

1. The protective lighting circuits will be so arranged that failure of any one lamp will not leave a large portion of the perimeter line or a major segment of a critical or vulnerable area in darkness.

2. Protective lighting will be on a separate/dedicated circuit to minimize the chances of accidents or overloads affecting security.

3. In addition, feeder lines will be located underground or, for overhead wiring, sufficiently inside the perimeter to minimize the possibility of sabotage or vandalism from outside the perimeter.

E. Power Sources.

1. Generator or battery-powered portable or stationary lights will be available for use by security personnel in case of complete power failures. Generators will be capable of operating for a minimum of four hours.

2. Alternate power sources will be tested at least monthly to ensure their efficiency and effectiveness and the tests will be recorded as determined locally. The duration of the tests will be dependent on the type and condition of the equipment, weather, and factors such as the mission and operational situation.

F. CCTV Lighting Requirements.

1. UFC 4-020-04FA and UFGS 26 55 53.00 10, "Exterior Lighting including Security and CCTV Application," provides a detailed discussion of CCTV-camera lighting requirements and guidelines for minimum lighting levels and lighting uniformity.

2. The following considerations apply when lighting systems are intended to support CCTV assessment or surveillance:

a. The camera's field of view.

b. Lighting intensity levels.

c. Maximum light-to-dark ratio.

d. Scene reflectance.

e. Daylight-to-darkness transitions.

f. Camera mounting systems relative to lighting.

g. The camera's spectral response.

h. The cold-start time.

i. The restrike time.

G. Replacing Lights.

1. The owner/user is responsible for identifying defective or burned out lights. The user will replace these lights within capability or notify Facilities within 24 hours for repair

2. DLA Police Officers are responsible for conducting nightly checks of installation/perimeter boundary light list, listing all discrepancies in the blotter, and the following day reporting the finding(s) to the Installation Facilities Management.

CHAPTER 6: ELECTRONIC SECURITY SYSTEMS (ESS)

A. General.

1. An overall site-electronic security system is comprised of three major sub-elements: detection, delay, and response. The detection sub-element includes intrusion detection, assessment, and entry control. An ESS is an integrated system that encompasses interior and exterior sensors; CCTV systems for assessing alarm conditions; electronic entry-control systems (EECSs); data-transmission media (DTM); and alarm reporting systems for monitoring, controlling, and displaying various alarm and systems information. Interior and exterior sensors and their associated communication and display subsystems are collectively called intrusion detection systems (IDS).

2. The use of leased or purchased commercial security equipment is authorized pending approval by DLA Installation Support, Security and Emergency Services.

3. Leasing arrangements will include a provision for Government retention of all wiring and cabling associated with the ESS after termination of the lease.

4. ESS maintenance and monitoring personnel must have at a minimum a completed National Agency Check with Inquiry, and been subjected to a trustworthiness determination in accordance with DoD 5200.2-R.

B. Use of ESS.

The decision to install an IDS will be based on requirements derived from DoD directive/instructions/manual to include UFGS 28 20 01.00 10, “Electronic Security System.” Prior to installation of an IDS, PLFA Commanders/Directors along with the Chief of Security and Emergency Services will consider the threat, vulnerabilities, in-depth security measures and shall perform a risk analysis.

C. General Description.

1. An ESS provides early warning of an intruder. This system will consist of hardware and software elements operated by trained security personnel. Systems must be configured to provide one or more layers of detection around an asset. Each layer shall be made up of a series of contiguous detection zones designed to isolate the asset and to control the entry and exit of authorized personnel and materials.

2. An ESS consists of sensors interfaced with electronic entry-control devices, CCTV, alarm reporting displays (both visual and audible), and security lighting. The situation shall be assessed by sending police or security forces to the alarm point. Alarm reporting devices and video monitors must be located in the security operations center.

D. Design Considerations.

1. A facility may require interior and exterior ESS elements, depending on the level of protection required. Applicable regulations, local threat, and design criteria will define the ESS's general requirements. For an existing ESS, hardware and software may need to be supplemented, upgraded, or completely replaced. A site layout (in which all assets are identified and located) is required.

2. The exterior and interior IDSs will be configured as layers of unbroken rings concentrically surrounding the asset. These rings will correspond to defensive layers that constitute the delay system. The first detection layer shall be located at the outermost defensive layer necessary to provide the required delay. Detection layers can be on a defensive layer, in the area between two defensive layers, or on the asset itself, depending on the delay required. For example, if a wall of an interior room provides sufficient delay for effective response to aggression, detection layers could be between the facility exterior and interior-room wall or on the interior-room wall. These would detect the intruder before penetration of the interior wall is possible.

3. Response and Delay.

a. When dealing with an ESS, the response time is defined as the time it takes the security force to arrive at the scene after an initial alarm is received at the security operations center. The total delay time is defined as the sum of all of the barriers' delay times, the time required to cross the areas between barriers after an intrusion alarm has been reported, and the time required accomplishing the mission and leaving the protected area.

b. An ESS's basic function is to notify security personnel that an intruder is attempting to penetrate, or has penetrated, a protected area in sufficient time to allow the response force to intercept and apprehend. To accomplish this, there must be sufficient physical delay between the point where the intruder is first detected and his objective.

c. When dealing with interior sensors, boundary sensors that detect penetration (such as structural-vibration sensors or passive ultrasonic sensors) provide the earliest warning of an attempted intrusion. This alarm is usually generated before the barrier is penetrated. This gives the security force advance notification of an attempted penetration, thus allowing the barrier's delay time to be counted as part of the total delay time. Door-position sensors and glass-breakage sensors do not generate an alarm until the barrier has been breached; therefore, the delay time provided by the barrier cannot be counted as part of the total delay time.

d. Volumetric motion sensors do not generate an alarm until the intruder is already inside the area covered by the sensors. Therefore, if these sensors are to be used to provide additional response time, additional barriers must be placed between the volumetric motion sensors and the protected asset. Point sensors, such as capacitance sensors and pressure mats, provide warning of attempted penetration only if they detect the intruder before access is gained to the protected area.

4. Basic Guidance.

a. An IDS is deployed in and around barriers. Voice communication links (radio, intercom, and telephone) with the response force are located in the security operations center. Designated personnel will man the operations center and will alert and dispatch response forces in case of an alarm.

b. Data for monitoring and controlling an ESS are gathered and processed in the security operations center where the operator interacts with information from the ESS components located at remote facilities. The ESS's alarm-annunciation computer and its DTM line-termination equipment will be located in a controlled area and provided with tamper protection. Supervisory personnel should permit changes to software only, and these changes should be documented. If redundant DTM links connect the central computer to the local processor, diverse paths should be used to route these links.

c. The preferred medium for transmitting data in an ESS is a dedicated fiber-optics system. It provides for communications not susceptible to voltage transients, lightning, electromagnetic interference, and noise. Additionally, the fiber optics will provide a measure of communication-line security and wide bandwidth for video signals and increased data-transmission rates.

E. ESS Effectiveness.

1. To be effective, an ESS should have the following basic components:

a. Intrusion-detection sensors.

b. Electronic entry-control devices.

c. CCTV. (Optional)

d. Alarm-annunciation system.

e. DTM.

2. After an alarm is sensed and information is displayed in the security operations center, the console operator must determine the cause of the alarm (intrusion, nuisance, environmental, or false). Timely assessment is required when determining its cause.

3. For a CCTV camera to be effective, the area it views must be adequately lighted. To correlate the alarms and cameras in a large system (more than 10 cameras) in a timely manner, a computer-based processing system must be used to select and display alarms and camera scenes for the operator.

F. Tamper Protection.

1. To minimize the possibility of someone tampering with circuitry and associated wiring, all sensor-related enclosures must be equipped with tamper switches. These switches must be positioned so that an alarm is generated before the cover has been moved enough to permit access to the circuitry of adjustment controls.

2. In addition, several types of sensors should be equipped with tamper switches to protect against being repositioned or removed. Security screens containing grid-wire sensors and vibration sensors that can be easily removed from a wall are examples of sensors that require tamper switches.

G. Access/Secure Mode.

1. During regular working hours, many of the interior sensors must be deactivated by placing the area in the access mode. For example, volumetric sensors in occupied areas must be deactivated to prevent multiple nuisance alarms caused by the normal movement of people. This can be done locally or remotely. However, when a sensor is placed in the access mode, its tamper-protection circuitry must remain in the activated or secure mode.

2. During nonworking hours when the facility is unoccupied, all sensors must be placed in the secure mode. Certain devices (such as duress-alarm switches, tamper switches, grid-wire sensors covering vent openings, and glass-breakage sensors) will always remain in secure mode.

3. The Chief, Security and Emergency Services/Chief, Security Services must ensure that selected sensors can be placed in an access mode (if required) and that certain types of sensors (such as duress and tamper switches) are configured so that they cannot be put in the access mode under any condition.

H. Perimeter Layout and Zoning.

1. A protected area's perimeter is usually defined by an enclosing wall or fence or a natural barrier such as water. For exterior sensors to be effective, the perimeter around which they are to be deployed must be precisely defined. In most applications, a dual chain-link-fence configuration will be established around the perimeter.

a. Typically, fences should be between 30 and 50 feet apart; as the distance increases, it is harder for an intruder to bridge the fences. If fence separation is less than 30 feet, some microwave and ported-coax sensors cannot be used. The area between fences (called the controlled area or isolation zone) may need to be cleared of vegetation and graded, depending on the type of sensor used.

b. Proper drainage is required to preclude standing water and to prevent the formation of gullies caused by running water after a heavy rain or melting snow.

c. Cleared areas are required inside and outside of the controlled area. These areas enhance routine observation, as well as sensor-alarm assessment, and minimize the protective cover available to a would-be intruder.

2. After the perimeter has been defined, the next step is to divide it into specific detection zones. The length of each detection zone is determined by evaluating the contour, the existing terrain, and the operational activities along the perimeter.

a. Detection zones should be long and straight to minimize the number of sensors or cameras necessary and to aid guard assessment if cameras are not used. It may be more economical to straighten an existing fence line than to create numerous detection zones in accommodating a crooked fence line.

b. Entry points for personnel and vehicles must be configured as independent zones. This enables deactivation of the sensors in these zones; that is, placing them in the access mode during customary working hours (assuming the entry points are manned) without having to deactivate adjacent areas.

3. The specific length of individual zones can vary around the perimeter. Although specific manufacturers may advertise maximum zone lengths exceeding 1,000 feet, it is not practical to exceed a zone length of 300 feet. If the zone is longer, it will be difficult for an operator using CCTV assessment or for the response force to identify the location of an intrusion or the cause of a false alarm.

4. When establishing zones using multiple sensors, coincident zones will be established, where the length and location of each individual sensor will be identical for all sensors within a given zone. If an alarm occurs in a specific zone, the operator can readily determine its approximate location by referring to a map of the perimeter. This also minimizes the number of CCTV cameras required for assessment and simplifies the interface between the alarm-annunciation system and the CCTV switching system.

I. Alarm-Annunciation System.

1. Status information from the various intrusion-detection sensors and entry-control terminal devices must be collected from the field and transmitted to the alarm-annunciation system in the Security Operations Center, where it is processed, annunciated, and acted on by security personnel.

2. The alarm-annunciation system should also interface with a CCTV system. There are typically two types of alarm-annunciation configurations available.

a. The simplest configuration, which is suitable for small installations, is the point-to-point configuration. With this configuration, a separate transmission line is routed from the protected area to the security operations center (see Figure 6-1).

b. The second, and more popular type, is a digital multiplexed configuration that allows multiple protected areas to communicate with the security operations center over a common data line. A block diagram of a typical multiplexed alarm-annunciation system is shown in Figure 6-2.

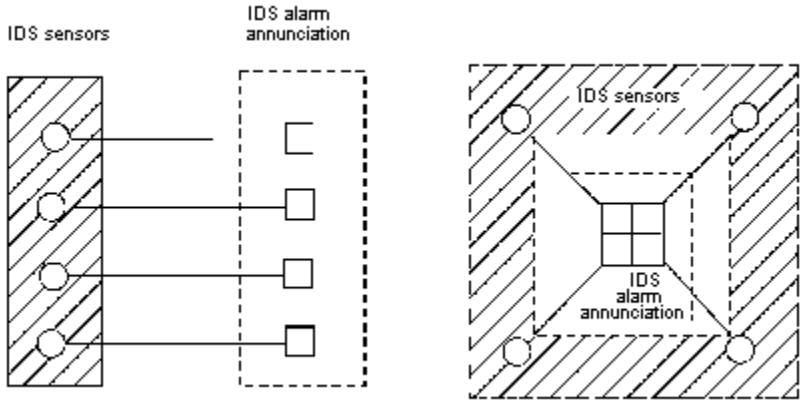

Figure 6-1. Typical Point-to-Point IDS

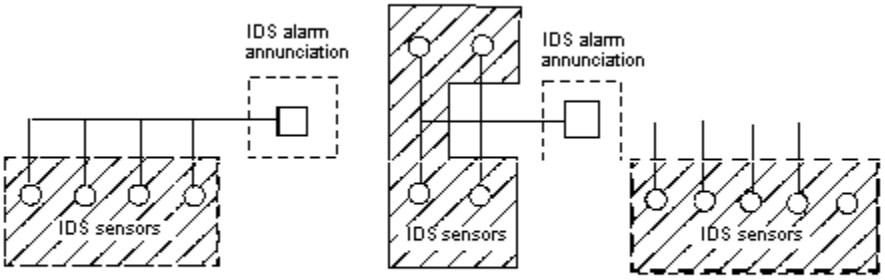

Figure 6-2. Typical Multiplexed IDS

3. Alarm-Annunciation Configuration. A block diagram of a typical alarm-annunciation system is shown in Figure 6-3. As shown in the figure, the central computer is the hub of the information flow. The central computer receives and displays alarm and device status information and sends operator-control commands to the ESS's local processors. It also interfaces with the CCTV system. For larger facilities, the management of the DTM communications tasks may be delegated to a separate communication processor so that the central computer can turn its full attention to interpreting the

incoming information and updating the control and display devices located at the security console (display, logging, control, and storage devices).

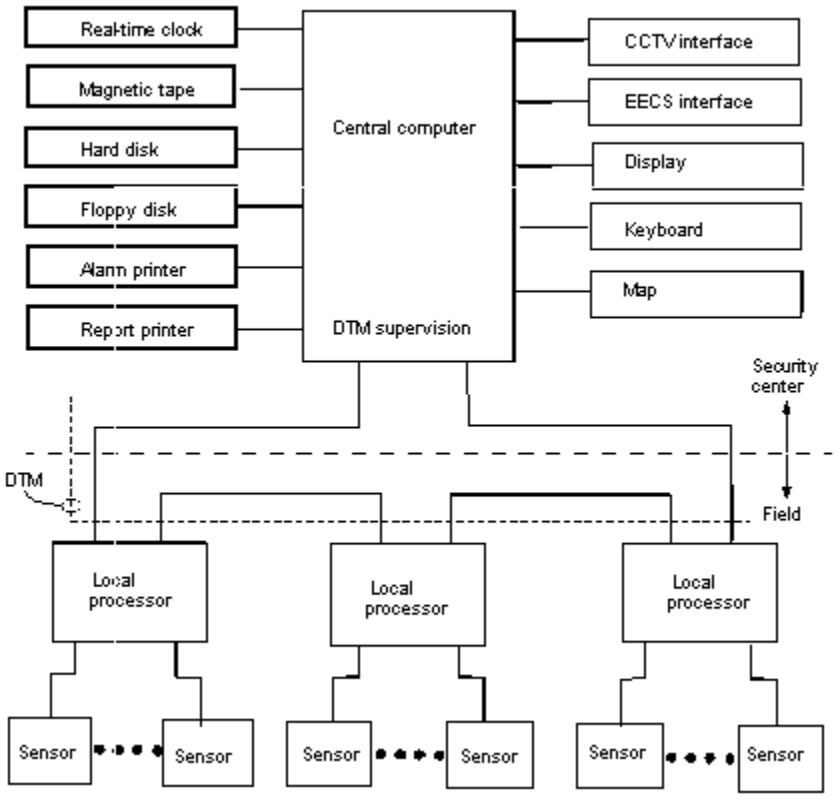

Figure 6-3. Typical IDS Alarm-Annunciation System

4. Operator Interface. The operator interacts with the alarm-annunciation system through devices that can be seen, heard, or touched and manipulated. Visual displays and printers should be used to inform the operator of an alarm or the equipment's status. Audible devices must be used to alert an operator to an alarm or the equipment's failure. Devices such as push buttons and keyboards permit an operator to acknowledge and reset alarms, as well as change operational parameters.

a. Visual displays. The type of display used to inform the operator visually of the ESS's status is determined locally based primarily by the system's complexity. Status information is usually displayed on monitors. Alphanumeric displays and map displays are seldom used. Monitors provide great flexibility in the type and format of alarm information that may be displayed. Both text and graphic information can be displayed in a variety of colors. Multiple alarms may also be displayed. If alarms are prioritized, higher-priority alarms may be highlighted by blinking, by using bold print or reverse video, or by changing colors. To assist the operator in determining the correct response, alarm-specific instructions may be displayed adjacent to the alarm information.

b. Audible alarm devices. In conjunction with the visual display of an alarm, the alarm-annunciation system must also generate an audible alarm. The audible alarm may be produced by the ringing of a bell or by the generation of a steady or pulsating tone from an electronic device. In any case, the audible alarm serves to attract the operator's attention to the visual-alarm display. A silence switch is usually provided to allow the operator to silence the bell or tone before actually resetting the alarm.

c. Logging devices. All alarm-system activity (such as a change of access/secure status, an alarm event, an entry-control transaction, or a trouble event) will be logged and recorded. Logged information is important not only for security personnel investigating an event, but also for maintenance personnel checking equipment performance for such causes as false and nuisance alarms. Most alarm-annunciation systems are equipped with logging and alarm printers. Log information shall be destroyed after 2 years per GRS 18, item 20..

d. Alarm printers. Alarm printers will be of the high-speed, continuous-feed variety. The printer provides a hard-copy record of all alarm events and system activity, as well as limited backup in case the visual display fails.

e. Report printers. Most ESSs include a separate printer (report printer) for generating reports using information stored by the central computer. This printer will usually be typical of those found in modern office environments.

f. Operator control. A means is required to transmit information from the operator to the system. The type of controls provided usually depends on the type of display provided. The following are consistent with the controls:

(1) Keypads consist of a numeric display system that will generally be provided with a 12-digit keypad and several function keys such as access, secure, acknowledge, and reset. The keypad enables an operator to key in numeric requests for the status of specific zones.

(2) Monitor-based systems are usually provided with a typewriter-type keyboard that enables an operator to enter more information using a combination of alphanumeric characters and function keys.

(3) An ESS may be equipped with enhancement hardware/devices to help the operator enter information or execute commands quickly. A mouse or a trackball are typical examples.

J. CCTV Interface.

If a CCTV assessment system is deployed with the ESS, an interface between the two is required. This interface allows CCTV system alarms (such as loss of video) to be displayed by the ESS's alarm-annunciation system. The interface also provides IDS alarm signals to the CCTV's video switcher so that the correct CCTV camera will be displayed on the CCTV monitors to allow real-time alarm assessment and video recording as required.

K. ESS Software.

1. The software provided with computer-based ESS alarm-annunciation systems should be one of three types—a standard operating system (Microsoft Windows); vendor-developed application programs; and/or user-filled, site-specific data structures.

a. System software. System software provided by the vendor must conform to accepted industry standards so that standard, follow-on maintenance and service contracts can be negotiated to maintain the central computer system.

b. Application software. The vendor-developed application programs are typically proprietary and include ESS monitoring, display, and entry-control capabilities.

c. User-filled data structures. These data structures are used to populate the site-specific database. Specific electronic address information, personnel access schedules, and normal duty hours are typically included in the site-specific database. The information may include preferred route descriptions for the response force, the phone number of the person responsible for the alarmed area, and any hazardous material that may be located in the alarmed area.

2. ESS software functions should include the following:

a. Alarm monitoring and logging. The software should provide for monitoring all sensors, local processors, and data communication links and notifying the operator of an alarm condition. All alarm messages should be printed on the alarm printer, archived, and displayed at the console. As a minimum, printed alarm data should include the date and time (to the nearest second) of the alarm and the location and type of alarm.

b. Alarm display. The software should be structured to permit several alarms to be annunciated simultaneously. A buffer or alarm queue should be available to store additional alarms until they are annunciated and, subsequently, acted upon and reset by the console operator.

c. Alarm priority. Alarm priority will be set according to Chapter 10, Designation and Protection of Secure Areas.

3. Reports. The application software should provide for generating, displaying, printing, and storing reports.

4. Passwords.

a. Software security will be provided by limiting access to personnel with authorized passwords assigned by a system manager. A minimum of three password levels shall be provided.

b. Additional security can be provided by programmed restrictions that limit the keyboard actions of logged-in passwords to the user ranks of system managers, supervisors, and console operators, as appropriate.

5. Operator Interface. The software should enable an operator with the proper password to enter commands and to obtain displays of system information. As a minimum, an operator should be able to perform the following functions through the keyboard or the keypad:

a. Log on by password to activate the keyboard.

b. Log off to deactivate the keyboard.

c. Request display of all keyboard commands that are authorized for the logged-in password.

d. Request display of detailed instructions for any authorized keyboard command.

e. Acknowledge and clear alarm messages.

f. Display the current status of any device in the system.

g. Command a status change for any controlled device in the system.

h. Command a mode change for any access/secure device in the system.

i. Command printouts of alarm summaries, status summaries, or system activity on a designated printer.

j. Add or delete ESS devices or modify parameters associated with a device.

L. Interior Intrusion Detection Sensors.

1. Interior intrusion detection sensors are devices used to detect unauthorized entry into specific areas or volumetric spaces within a building. These sensors are usually not designed to be weatherproof or rugged enough to survive an outdoor environment. Therefore, this type of sensor should not be used outdoors unless described by the manufacturer as suitable for outdoor use.

2. Interior intrusion detection sensors generally perform one of three detection functions—detection of an intruder penetrating the boundary of a protected area, detection of intruder motion within a protected area, and detection of an intruder touching or lifting an asset within a protected area. Therefore, interior sensors are commonly classified as boundary-penetration sensors, volumetric motion sensors, and point sensors.

3. Although duress switches are not intrusion detection sensors, they are included in this discussion because they are usually wired to the same equipment that monitors the interior intrusion-detection sensors.

a. Duress-alarm devices may be fixed or portable. Operations and security personnel use them to signal a life-threatening emergency. Activation of a duress device will generate an alarm at the alarm-monitoring station.

b. Because of the nature of the alarm, duress devices should never annunciate at the point of threat. Duress alarms at the alarm-monitoring station must annunciate at an alternate location (i.e., main gate, command post).

M. Exterior Intrusion Detection Sensors.

1. Exterior intrusion detection sensors are customarily used to detect an intruder crossing the boundary of a protected area. They can also be used in clear zones between fences or around buildings, for protecting materials and equipment stored outdoors within a protected boundary, or in estimating the probability of detection (PD) for buildings and other facilities.

2. Exterior sensors must be designed to operate in outdoor environmental conditions. The detection function must be performed with a minimum of unwanted alarms such as those caused by wind, rain, ice, standing water, blowing debris, animals, and other sources. Important criteria for selecting an exterior sensor are the PD, the sensor's susceptibility to unwanted alarms, and the sensor's vulnerability to defeat.

3. As with interior sensors, tamper protection, signal-line supervision, self-test capability, and proper installation make exterior sensors less vulnerable to defeat. Because signal-processing circuitry for exterior sensors is generally more vulnerable to tampering and defeat than that for interior sensors, it is extremely important that enclosures are located and installed properly and that adequate physical protection is provided. Several different types of exterior intrusion detection sensors are available. They can be categorized as:

a. Fence sensors.

b. Buried line sensors.

c. Line-of-sight (LOS) sensors.

d. Video motion sensors.

N. Electronic Entry Control

1. The function of an entry-control system is to ensure that only authorized personnel are permitted into or out of a controlled area. Entry can be controlled by locked fence gates, locked doors to a building or rooms within a building, or specially designed portals.

2. These means of entry control can be applied manually by guards or automatically by using entry-control devices.

a. In a manual system, guards verify that a person is authorized to enter an area, usually by comparing the photograph and personal characteristics of the individual requesting entry.

b. In an automated system, the entry-control device verifies that a person is authorized to enter or exit. The automated system usually interfaces with locking mechanisms on doors or gates that open momentarily to permit passage.

3. Coded Devices.

a. Coded devices operate on the principle that a person has been issued a code to enter into an entry-control device. This code will match the code stored in the device and permit entry.

b. Depending on the application, a single code can be used by all persons authorized to enter the controlled area or each authorized person can be assigned a unique code.

c. Group codes are useful when the group is small and controls are primarily for keeping out the general public. Individual codes are usually required for control of entry to more critical areas.

d. Coded devices verify the entered code's authenticity, and any person entering a correct code is authorized to enter the controlled area. Electronically coded devices include electronic and computer-controlled keypads.

4. Credential Devices. A credential device may be used to identify a person having legitimate authority to enter a controlled area. A DLA-coded credential (plastic card or key) contains a prerecorded, machine-readable code. Accepted cards for DLA use are:

a. Magnetic-Stripe Card: A strip of magnetic material located along one edge of the card is encoded with data (sometimes encrypted). The data is read by moving the card past a magnetic read head.

b. Wiegand-Effect Card. The Wiegand-effect card contains a series of small-diameter, parallel wires about one-half inch long, embedded in the bottom half of the card. The wires are manufactured

from ferromagnetic materials that produce a sharp change in magnetic flux when exposed to a slowly changing magnetic field. This type of card is impervious to accidental erasure. The card reader contains a small read head and a tiny magnet to supply the applied magnetic field. It usually does not require external power.

c. Proximity Card. A proximity card is not physically inserted into a reader; the coded pattern on the card is sensed when it is brought within several inches of the reader. Several techniques are used to code cards. One technique uses a number of electrically tuned circuits embedded in the card. Data are encoded by varying resonant frequencies of the tuned circuits. The reader contains a transmitter that continually sweeps through a specified range of frequencies and a receiver that senses the pattern of resonant frequencies contained in the card. Another technique uses an integrated circuit embedded in the card to generate a code that can be magnetically or electrostatically coupled to the reader. The power required to activate embedded circuitry can be provided by a small battery embedded in the card or by magnetically coupling power from the reader.

d. Laser Card. The optical memory card, commonly called the laser card, uses the same technology developed for recording video and audio disks for entertainment purposes. Data is recorded on the card by burning a microscopic hole (using a laser) in a thin film covering the card. Data is read by using a laser to sense the hole locations. The typical laser card can hold several megabytes of user data.

e. Smart Card. A smart card is embedded with a microprocessor, memory, communication circuitry, and a battery. The card contains edge contacts that enable a reader to communicate with the microprocessor. Entry-control information and other data may be stored in the microprocessor's memory.

f. Bar Code. A bar code consists of black bars printed on white paper or tape that can be easily read with an optical scanner. This type of coding is not widely used for entry-control applications because it can be easily duplicated. It is possible to conceal the code by applying an opaque mask over it. In this approach, an infra-red (IR) scanner is used to interpret the printed code. For low-level security areas, the use of bar codes can provide a cost-effective solution for entry control. Coded strips and opaque masks can be attached to existing ID badges, alleviating the need for complete badge replacement.

5. **Biometric Devices.** As technology develops, characteristics such as fingerprints, hand geometry, voiceprints, handwriting, and retinal blood-vessel patterns may be used for controlling entry. Organizations utilizing biometric devices for access control will be aware of the privacy concerns such technology raises for the affected population and the potential requirements associated with collecting PII. While current biometric access technologies are effective for applications seeking to identify few known individuals, the privacy and cost/benefit for newer applications of biometric devices should be evaluated prior to adoption.

6. **Enrollment.** All entry-control systems must provide a means of entering, updating, and deleting information about authorized individuals into the system's database files. When credential devices are used, all authorized users must be provided with an appropriate credential. A means should also be provided to disenroll a person quickly without having to retrieve a credential. When using biometric devices, additional enrollment equipment will be required.

O. Data Transmission.

1. A critical element in an integrated ESS is the DTM that transmits information from sensors, entry-control devices, and video components to display and assessment equipment. A DTM link is a path for transmitting data between two or more components (such as a sensor and alarm reporting system, a card

reader and controller, a CCTV camera and monitor, or a transmitter and receiver). The DTM links connect remote ESS components to the security operations center.

2. Chiefs, Security and Emergency Services/Chiefs, Security Services must ensure an effective DTM link that provides rapid and reliable transmission media, transmission technique, associated transmission hardware, and degree of security to be provided for the communication system.

3. Although the preferred medium for transmitting data in an ESS is a dedicated fiber-optics system, security managers have the option of using a number of different media in transmitting data between elements of an IDS, an EECS, and a CCTV system. These include wire lines, coaxial cable, fiber-optic cable, and radio frequency (RF) transmission.

a. Fiber optics. Fiber optics uses the wide bandwidth properties of light traveling through transparent fibers. Fiber optics is a reliable communication medium best suited for point-to-point, high-speed data transmission. Fiber optics is immune to RF electromagnetic interference and does not produce electromagnetic radiation emission. The preferred DTM for an ESS is fiber-optic cables unless there are justifiable economic or technical reasons for using other types of media.

b. Wire line. Wire lines are twisted pairs that consist of two insulated conductors twisted together to minimize interference by unwanted signals.

c. Coaxial cable. Coaxial cable consists of a center conductor surrounded by a shield. The center conductor is separated from the shield by a dielectric. The shield protects against electromagnetic interference.

d. RF transmission. Modulated RF can be used as a DTM with the installation of radio receivers and transmitters. An RF transmission system does not require a direct physical link between the points of communication, and it is useful for communicating over barriers such as bodies of water and heavily forested terrain. A disadvantage is that the signal power received depends on many factors (including transmission power, antenna pattern, path length, physical obstructions, and climatic conditions). Also, RF transmission is susceptible to jamming and an adversary with an appropriately tuned receiver has access to it. The use of RF will be coordinated with the communications officer to avoid interference with other existing or planned facility RF systems.

4. There are two basic types of communication links—point-to-point and multiplex lines.

a. A point-to-point link is characterized by a separate path for each pair of components. This approach is cost effective for several component pairs or when a number of scattered remote areas communicate with a single central location.

b. The multiplex link, commonly referred to as a multidrop or multipoint link, is a path shared by a number of components. Depending on the number and location of components, this type of configuration can reduce the amount of cabling required. However, the cost reduction from reduced cabling is somewhat offset by costs of equipment required to multiplex and demultiplex data.

5. Data links used to communicate the status of ESS devices or other sensitive information to the security operations center must be protected from possible compromise. Attempts to defeat the security system may range from simple efforts to cut or short the transmission line to more sophisticated undertakings, such as tapping and substituting bogus signals. Data links can be made more secure by physical protection, tamper protection, line supervision, and encryption.

P. CCTV for Alarm Assessment and Surveillance.

1. Chiefs, Security and Emergency Services/Chiefs, Security Services must ensure a properly integrated CCTV assessment system provides a rapid and cost-effective method for determining the cause of intrusion alarms. It is important to recognize that CCTV alarm-assessment systems and CCTV surveillance systems perform separate and distinct functions.

a. The alarm-assessment system is designed to respond rapidly, automatically, and predictably to the receipt of ESS alarms at the security operations center.

b. The surveillance system is designed to be used at the discretion of and under the control of the security operations center's console operator.

c. When the primary function of the CCTV system is to provide real-time alarm assessment, the design should incorporate a video-processing system that can communicate with the alarm-processing system.

2. CCTV assessment system should typically have the following characteristics:

a. Assets requiring ESS protection.

b. A need for real-time alarm assessment.

c. Protected assets spaced some distance apart.

3. Figure 6-4 below shows a typical CCTV system configuration. A typical site will locate CCTV cameras:

a. Outdoors, along site-perimeter isolation zones.

b. Outdoors, at controlled access points (sally ports).

c. Outdoors, within the protected area, and at viewing approaches to selected assets.

d. Indoors, at selected assets within the protected area.

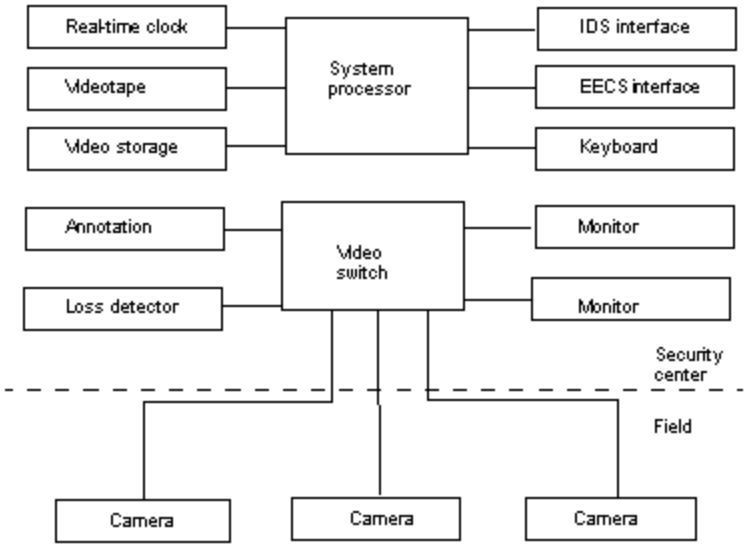

Figure 6-4. Typical CCTV System

4. The security console will be centrally located in the security operations center. The CCTV monitors and the ancillary video equipment will be located at this console, as will the ESS alarm-processing and -annunciation equipment.

Q. Video Processing and Display Components.

1. Psychological testing has demonstrated that the efficiency of console-operator assessment improves as the number of console monitors is reduced, with the optimum number being four to six monitors. Effectiveness is also enhanced by the use of alarm-correlated video.

2. Major components of the video-processor system should consist of the video switcher, the video-loss detector, the alarm-processor communication path, the master video-sync generator, video recorders, and monitors.

a. Video switchers. Video switchers are required when the number of cameras exceeds the number of console monitors or when a monitor must be capable of selecting video from one of many sources. Video switchers are capable of presenting any of multiple video images to various monitors, recorders, and so forth.

b. Video-loss detector. Video-loss detectors sense the continued integrity of incoming camera signals.

c. ESS interface and communication path. There must be a means of rapid communication between the ESS alarm-annunciation and video-processor systems. The alarm processor must send commands that cause the video switcher to select the camera appropriate for the sensor reporting an alarm. The video-processor system must report system tampering or failures (such as loss of video) to the alarm processor. The path should also pass date-and-time synchronizing information between processors so that recorded video scenes and printed alarm logs are properly correlated.

d. Master video-sync generation and distribution. Master video sync includes a crystal-controlled timing generator, distribution amplifiers, and a transmission link to each camera.

e. Video recorders. Video recorders (videocassette or digital) provide the means to record alarm-event scenes in real time for later analysis. A recorder typically receives its input through dedicated video-switcher outputs. To support recorder playback, the recorder output is connected to a dedicated switcher input and must be compatible with the switcher-signal format. In addition, the recorder receives start commands from the switcher, and compatibility must exist at this interface.

f. Monitors. Monitors are required to display the individual scenes transmitted from the cameras or from the video switcher. In alarm-assessment applications, the monitors are driven by dedicated outputs of the video switcher and the monitors display video sources selected by the switcher. For security-console operations, the 9-inch monitor is the smallest screen that should be used for operator recognition of small objects in a camera's field of view.

R. CCTV Application Guidelines.

1. Site-specific factors must be taken into consideration in selecting components that comprise a particular CCTV system. The first is the system's size in terms of the number of cameras fielded, which is the minimum number needed to view all ESS sensor-detection fields and surveillance cameras. Another factor is that some CCTV cameras may require artificial light sources. Finally, there are CCTV-system performance criteria and physical, environmental, and economic considerations.

2. **Scene Resolution**.

a. The level to which video details can be determined in a CCTV scene is referred to as resolving ability or resolution. It is generally accepted that for assessment purposes, three resolution requirements can be defined. In order of increasing resolution requirements, they are detection, recognition, and identification.

(1) Detection is the ability to detect the presence of an object in a CCTV scene.

(2) Recognition is the ability to determine the type of object in a CCTV scene (animal, blowing debris, or crawling human).

(3) Identification is the ability to determine object details (a particular person, a large rabbit, a small deer, or tumbleweed).

b. A CCTV assessment system should provide sufficient resolution to recognize human presence and to detect small animals or blowing debris. Given an alarmed intrusion sensor, it is crucial that the console operator be able to determine if the sensor detected an intruder or if it is simply responding to a nuisance condition.

3. **Design Guidelines.** Because the design and application of CCTV systems are quite complex, security personnel must work very closely with professionals who are abreast of the current state-of-the-art systems. Some of the general design guidelines include the following:

a. System familiarity. Before designing an effective CCTV assessment system, security personnel must be familiar with the ESS's sensor placement and the detection field's shape.

b. CCTV camera placement and lighting. The placement of exterior cameras requires more attention than that of interior cameras because of weather and illumination extremes. The field-of-view alignment, illumination range, and balanced lighting are major design factors. Exterior CCTV design considerations include environmental housings, camera mounting heights, system types, and so forth. Indoor placement of CCTV require a balancing of security and privacy interests. Prior to placement of any CCTV camera where revealing personal information occurs on a regular basis, e.g., bathroom stalls, dressing rooms, showers, etc., a balancing of security against any privacy interests should be made. If the decision to monitor such an area is made, then clear notices should be provided that such areas are being monitored via CCTV for security purposes so that individuals are making an informed decision. Indoor design considerations include the mounting location and tamper detection. The layout for indoor alarm-assessment cameras is subject to three constraints:

(1) The camera's location should enclose the complete sensor detection field in the camera's field of view.

(2) Lighting that is adequate to support alarm assessment will be provided.

(3) Protection from tampering and inadvertent damage by collision during normal area operations will be provided.

S. Additional Requirements.

1. Auxiliary Power Source. If an ESS is to be effective, the system should remain in continuous operation during the activity's non-operational hours. Each system must be capable of operating from an auxiliary power source. The time requirement for such operational capability must be evaluated in each case dependent upon such factors as alternate power supplies, maintenance support, and hours of active operation.

a. Auxiliary power sources for ESS will be tested monthly.

b. Records of such tests will be maintained by the Facility Engineer and inspected by the Chiefs, Security and Emergency Services/Chiefs, Security Services semiannually. Information shall be destroyed 2 years after final entry.

2. For unclassified areas and assets, plans and diagrams showing the location and technical data of installed systems, signal transmission lines, and control units will be marked "FOR OFFICIAL USE ONLY." Access to such plans and diagrams will be strictly limited to those with a "need to know."

3. For classified areas and assets, system plans and diagrams will be marked and protected in accordance with DoD 5200.1-R, *Information Security Program*. Operating and maintenance personnel must be cleared for access to classified information at the level necessary for the area concerned.

4. Alarm installation and maintenance will be accomplished by U.S. citizens who have been subjected to a trustworthiness determination in accordance with DoD 5200.2-R. Additionally, the alarm monitor station will be supervised continuously by U.S. citizens who also have been subjected to a trustworthiness determination in accordance with DoD 5200.2-R.

5. The alarm receiving area will be designated a Controlled Area and will give adequate protection to monitor personnel, as this will be a prime target for an intruder. Provision for emergency assistance to this area will be established and appropriate measures will be employed to ensure that monitor personnel

maintain the system's integrity. Admittance to this area will be restricted to supervisory and maintenance personnel.

6. Personnel on duty at the alarm receiving area will record all alarms and actions involving the IDS.

a. Entries should include the following:

(1) Date, time, and prevailing weather conditions.

(2) Name of person recording an alarm signal.

(3) Location of the alarm.

(4) Action taken in response to alarm.

(5) Total time that was required by responding personnel to arrive at the scene of an alarm.

(6) Cause of the alarm.

(7) Tests of alarms.

(8) Malfunctions, including nuisance alarms.

(9) Servicing and maintenance of detection systems.

b. Those facilities having automated systems need not duplicate information recorded in the system.

c. Disposition of records/files. Alarm record entries: Information shall be destroyed 2 years after final entry per GRS 18, item 20a.

7. A locally developed identity verification and duress code will be used with each IDS to ensure positive identification of persons entering or exiting alarmed structures and opening or closing alarmed containers. These codes will be:

a. Developed and distributed by the Chief, Security and Emergency Services/Chief, Security Services.

b. Marked and protected "For Official Use Only."

c. Varied for each alarmed area.

d. Changed quarterly at a minimum, unless compromised, in which case the codes will be changed immediately.

e. Used with a roster of authorized personnel provided to the Security Manager by the supervisor of the alarmed area.

8. The IDS will be tested quarterly and duress alarms will be tested monthly to ensure component parts are operating properly.

a. Results of these tests will be recorded. Information pertaining to alarm record entries shall be destroyed 2 years after final entry per GRS 18, item 20a.

b. The Chief, Security and Emergency Services/Chief, Security Services and custodian of the facility or resource protected by the IDS will arrange procedures for these tests. IDS tests may occur during normal duty opening or closing of the protected area.

9. Disposition of routine surveillance footage. Routine surveillance footage shall be destroyed when 6 months old per GRS 21, item 18.

CHAPTER 7: KEY AND LOCK CONTROL

A. General.

1. A key and lock control system encompassing all locks and keys used to secure government property will be established for all DLA Activities. In designing the system, planners must recognize that locks are delay devices only. Lock adequacy and effectiveness will only be as good as the controls placed over them. The key and lock control system supplements other security measures used to control access and are essential for the safeguarding of facilities and material. For additional information refer to Chapter 12 of this manual, "Arms, Ammunition, and Explosives (AA&E)," Key and Lock Control.

2. DLA Activities that are tenants on military installations, Government-owned, or privately-owned buildings will comply with the provisions of this section commensurate with existing lease arrangements, security support agreements, and/or Memoranda of Understanding (MOU).

3. A Key Control Officer will be designated in writing by the PLFA Commander/Director. The designee will be concerned with the supply of locks and how they are stored, the handling of keys, record files, investigation of lost keys, maintenance and operation of key repositories, and the overall supervision of the key and lock control system. The Chief, Security and Emergency Services/Chief, Security Services will not be the Key Control Officer.

4. The Chief, Security and Emergency Services/Chief, Security Services will ensure the following is accomplished:

a. Advise the PLFA Commander/Director, the Key Control Officer, and key custodians on all matters relating to key and lock control.

b. Provide for inspection of control systems.

c. Provide for inspection of locking devices during off duty hours by security personnel.

d. Include key and lock control procedures in regular Security Education and Awareness Training sessions.

B. Security and Control Measures.

All keys within the key and lock control system must be kept under continuous accountability. This will be accomplished as follows:

1. The number of individuals authorized to draw keys will be kept to the absolute minimum commensurate with security and operational requirements. Flexitime will not be the sole justification for key issuance.

2. Master keys and operating keys to security areas will not be issued for personal retention or removal from the activity. This restriction also applies to keys that unlock repositories that contain keys to security areas.

3. When keys are not in use, they will be secured in containers of at least 20-gauge steel or material of equivalent strength. Key repositories will be attached to the structure to prevent easy removal and

located in buildings or rooms with structural features that forestall illegal entry. During off duty hours, the building will be locked with an approved locking device. Key repositories will be so located that they are under the surveillance of operating personnel during duty hours. Repositories will be kept locked except to issue or return keys or to conduct inventories. Separate key repositories will be maintained for operating and duplicate keys.

4. Operating and duplicate keys that control access to repositories containing keys to security areas (less utility areas), will be controlled from, and when not in use, stored in central key repositories under 24-hour control of the activity. Keys to utility areas will be controlled by the Facility Engineer.

5. Keys to administrative offices, desks, lockers, etc., which are not of security interest should not be included in the security Key and Lock Control Program however; all keys must be part of a key control inventory.6. DLA Form 1610, *Key Repository Index*, will be maintained for each repository within the key and lock control system. The Index will be kept inside the repository to which it pertains and will be used as the basis for inventories of keys controlled from the repository by individual key serial number.

6. DLA Form 1610a, *Key Repository Accountability Record*, will be used to maintain accountability of the keys in each repository.

7. DLA Form 1610b, *Delegation of Authority-Key Control*, will be used to authorize personnel to sign for keys. Designations of individuals authorized to sign for repository keys will be signed by an individual at the division level or higher. Several individuals may be listed on the same form provided they are all authorized to sign for all keys listed on the form. The DLA Form 1610b will expire 1 year from signature date.

8. DLA Form 1610c, *Key Control Register*, will be used by all repository custodians to record the issue and turn-in of keys. A separate DLA Form 1610c will be maintained for each repository. When not in use, DLA Form 1610c will be locked inside the repository to which it pertains. All keys removed from the repository will be recorded on the DLA Form 1610c.

9. All keys and padlocks within the key control system, to include keys issued for personal retention, will be physically inventoried by serial number, at least once every 6 months. A record of the inventory will be maintained by the Key Control Officer until completion of the next scheduled inventory.

10. Padlocks not in use will be secured, along with the corresponding keys, in a locked container that meets the requirements of a key repository. Access to the container will be controlled in the same manner as for key repositories.

11. Under no circumstances will locks be left hanging open on a hasp, staple, hook, or other device. In all cases, locks will be relocked to the staple immediately after opening and the key will be removed.

12. All combinations to key repositories storing keys to security areas will be changed at least once every 12 months, or upon the reassignment or departure of an individual with knowledge of the combination or upon compromise, whichever occurs first.

13. All combinations to safes or vaults designed for classified storage but which are used to store unclassified Government property will be changed in accordance with the DLA Information Security Manual (DLAI 6304).

14. The Chief, Security and Emergency Services/Chief, Security Services is not responsible for changing combinations on locking devices. Key Custodians will change their combinations in accordance with the manufacturer's instructions or through a maintenance contract.

15. Standard Form 700, *Security Container Information*, and Standard Form 702, *Security Container Check Sheet*, will be used in conjunction with each combination lock used to secure controlled items, funds, evidence, or other items.

16. Installation employees assigned to maintain or service locks within the Key and Lock Control Program will be approved by the Chief, Security and Emergency Services/Chief, Security Services. The positions of these employees will be designated noncritical sensitive and the appropriate investigations will be conducted.

C. Records.

Records will be maintained in accordance with GRS 18, item 16b, destroy 6 months after turn-in of key, lock, combination change, etc,, and will include the following information:

1. Total number of keys and locks under control, including lock cores, if any.

2. Number of keys issued for personal retention and the names of persons to whom keys have been issued.

3. Number of keys on hand.

4. Number of locks in use.

5. Number of reserve locks/keys.

D. Automated Key Control Systems.

An automated key control system may be used to store and control issue of security keys. The system should have sufficient controls built into it to provide the same or better security than the manual system described above. Completion of forms and reports mentioned above is not necessary if the system can generate the same information. At a minimum, the system should have the following characteristics:

1. Within 24 hours of notification, have the capability to remove access of personnel who have been terminated, resigned, transferred, or no longer have access to the areas that the keys unlock..

2. Register an alarm at the security operations center after 3 unsuccessful attempts to retrieve a key.

3. Register an alarm at the security operations center upon attempts to tamper with or defeat the system.

4. Register an alarm at the security operations center upon attempts to retrieve or return a key outside of normal duty hours.

5. Have the capability to limit read/write authority to the database. Read/write authority should be limited to the minimum number necessary for efficient and effective operations.

E. Local Procedures.

Local procedures may be developed and must include:

1. Location of key depositories.

2. Keys (by building, area, or cabinet number) to be turned in to each depository.

3. Matrix for marking or tagging keys for ready identification.

4. Method of control of issue and receipt of keys; to include identification of personnel authorized possession of keys.

5. Action required if keys are lost, stolen, or misplaced.

6. Frequency and method of lock rotation.

7. Emergency keys which would be readily available to the security supervisor.

8. Other controls as deemed necessary.

F. Seals.

Additional information on seals may be found in Chapter 4, Loss/Crime Prevention.

CHAPTER 8: SAFES AND STORAGE EQUIPMENT

A. Physical Protection and Storage of Materials.

Many types of storage equipment are used to store classified and sensitive information, weapons, controlled substances, valuable equipment, and negotiable documents or funds. Only equipment described in this section or specifically approved by DLA Installation Support, Security and Emergency Services should be used to safeguard such material when required by regulation or a risk assessment justifies the additional protection.

B. General Services Administration (GSA)-Approved Security Containers.

1. Federal Specifications. Federal specifications for security containers are developed by the Interagency Advisory Committee on Security Equipment, which also advises the GSA on security equipment listed in the FSS. Security containers furnished under the Federal specifications are tested, inspected, and approved for listing on an applicable qualified products list (QPL). The products are removed from the QPL whenever the specifications are changed to improve the product quality. These changes to the specifications are usually the result of constant testing and/or the development of new entry techniques. Security container manufacturers and prices of equipment approved by the GSA are listed in Federal Supply Schedule (FSS) Group 71 Part III E.

2. GSA Labels. A security container approved by GSA for storing classified information will bear a "General Services Administration Approved Security Container" label affixed to the front face and a "Test Certification" label affixed to the internal side of the door. Older containers will normally have only the test label located inside of the control drawer; however, the label may be missing from some containers as a result of age, damage, rehabilitation, or other modification. GSA Approved Class 5 and Class 6 containers produced after March 1991 and certified under the revised Federal specifications for increased surreptitious and covert protection bear a red "GSA Approved" label in lieu of the former black label. Black “GSA Approved” labels were issued on safes from 1962 until 1991 meeting previous Federal specifications.

3. Classes of GSA Approved Security Containers.

a. *Class 1*. The Class 1 security container is insulated for fire protection. The protection provided is:

30 man-minutes against surreptitious entry
10 man-minutes against forced entry
1 hour protection against fire damage to contents
20 man-hours against manipulation of the lock
20 man-hours against radiological attack

b. C*lass 2*. The Class 2 security container is insulated for fire protection. The protection provided is:

20 man-minutes against surreptitious entry
1 hour protection against fire damage to contents
5 man-minutes against forced entry

20 man-hours against manipulation of the lock
20 man-hours against radiological attack

c. *Class 3*. The Class 3 is an uninsulated security container, and the protection provided is:

20 man-minutes against surreptitious entry
20 man-hours against manipulation of the lock
20 man-hours against radiological attack
No forced entry requirement

d. C*lass 4.* The Class 4 is an uninsulated security container, and the protection provided is:

20 man-minutes against surreptitious entry
5 man-minutes against forced entry
20 man-hours against manipulation of the lock
20 man-hours against radiological attack

e. *Class 5.* The Class 5 is an uninsulated security container, and the protection provided is:

20 man-hours against surreptitious entry (increased from 30 man-minutes on containers produced after March 1991)
10 man-minutes against forced entry
30 man-minutes against covert entry (added to containers produced after March 1991)

f. *Class 6*. The Class 6 is an uninsulated security container, and the protection provided is:

20 man-hours against surreptitious entry (increased from 30 man-minutes on containers produced after March 1991)
No forced entry test requirement
30 man-minutes against covert entry (added to containers produced after March 1991)

4. Models of GSA-Approved Security Containers.

a. Security Filing Cabinets.

(1) A variety of security filing cabinets are manufactured in both Class 5 and Class 6 models. Security filing cabinets are available in single, two, four, and five drawers and in both letter size and legal size models.

(2) Class 1, 2, 3, and 4 security containers have not been listed in the FSS for a number of years.

b. Map and Plan Security Containers. Map and Plan Security Cabinets are manufactured in both Class 5 and Class 6 models. In addition to map and plan holders, this container is also available with various drawers, adjustable shelves, and in a weapons configuration for either rifles or pistols.

C. Record Safes Designed for Fire Protection.

A labeling service has been established by the Underwriter's Laboratory (UL) to define the level of fire protection each safe can be expected to provide. Prior to 1972, the UL designations used an alpha designation that was the same as the Safe Manufacturers National Association (SMNA). Both the former UL and SMNA designations are listed below with the current equivalent UL designation. Fire protection container manufacturers and prices of equipment approved by the GSA are listed in FSS Group 71 Part III.

1. Fire-Resistant Safes. There are three classes of fire-resistant safes. All three classes must pass three tests - fire endurance, explosion, and impact. During the fire endurance test, the inside temperature of a safe cannot exceed 350° F at any time during the test. At the end of the test, all papers inside a safe must be entirely legible and unsinged.

a. *Class 350-4 Hours (Former UL and SMNA Classification ("A").* A specimen safe containing papers and records is placed in a testing furnace and the temperature is raised through a standard curve until it is 2,000ºF at the end of four hours.

b. *Class 350-2 Hours (Former UL and SMNA Classification "B").* A specimen safe containing papers and records is placed in a testing furnace and must withstand two hours of exposure to heat reaching 1,850°F.

c. *Class 350-1 Hour (Former UL and SMNA Classification "C").* A specimen safe containing papers and records is placed in a testing furnace for a one-hour exposure to heat reaching 1,700°F.

2. Insulated Filing Devices. Insulated filing devices afford considerably less protection for records than the three levels of fire-resistant containers discussed above. The thermocouple devices to measure interior heat during the tests are located in the center of the interior compartment, and the insulated filing devices are not drop tested. As it is possible to confuse the 350-1 Insulated Filing Device with the 350-1 Fire-Resistant Safe, the label should be carefully noted.

a. C*lass 350-1 Hour (Former UL and SMNA Classification "D").* A specimen-filing device is placed in a testing furnace and is heated to temperatures reaching 1,700°F, for one hour.

b. *Class 350-1/2 Hour (Former UL and SMNA Classification "E").* A specimen-filing device is heated for one-half hour to a temperature reaching 1,550°F in a test furnace.

3. Insulated Record Containers. Because information technology (IT) records, such as magnetic storage media, begin to deteriorate at 150° F with humidity levels of more than 85 percent, Fire-Resistant Safes and Insulated Filing Devices should not be used to protect these types of records. To meet this requirement, a container that has been described as a "safe within a safe" was designed. This container has a sealed inner insulated repository in which the IT material is stored and an outer safe protected by a heavy wall of insulation. This type of container has been designed to protect IT records against 150°F temperature and 85 percent humidity for the period specified. Insulated Record Containers are labeled by UL as follows:

a. Insulated Record Container, Class 150-4 Hour

b. Insulated Record Container, Class 150-3 Hour

c. Insulated Record Container, Class 150-2 Hour

d. Insulated Record Container, Class 150-1 Hour

D. Burglary-Resistant Safes.

Containers designed for burglary protection are classified in accordance with test data and specifications that conform to requirements of the UL. Burglary-resistant equipment will resist an attack by tools, torch, or explosives in proportion to their construction specifications. Burglary-resistant container manufacturers and prices of equipment approved by the GSA are listed in the FSS Group 71 Part III.

1. UL Ratings. Safes undergo severe testing before receiving ratings from UL. The meaning of the various label designations resulting from the UL test are described below.

a. TL-15 or TL-30. The TL-15 or TL-30 signifies a combination-locked steel container offering a limited degree of protection against expert burglary with common mechanical or electrical tools. The container must successfully resist entry for a net working time of 15 or 30 minutes.

b. TRTL-30 or TRTL-60. The TRTL-30 or TRTL-60 signifies a combination-locked steel safe designed and tested to give protection against 30 or 60 minutes of attack with common electrical and mechanical tools, cutting torches, and any combination of these techniques. A successful attack consists of opening the door or making a two-inch square hole entirely through the door or front face.

c. TXTL-60. The TXTL-60 signifies a combination locked steel chest that offers 60 minutes of protection against an expert burglary attack using common hand tools, cutting torches, high explosives, and any combination of these techniques. A successful attack consists of opening the door or making a two-inch square hole entirely through the door or body.

2. Applications. Burglary resistant safes may be useful in establishing protection of valuable equipment, controlled substances, and negotiable documents or funds. The cost of any proposed container should always be compared with the protection required for the items being safeguarded. For example, it would be an unrealistic expenditure of funds to purchase a burglary-resistant safe for the sole purpose of storing a $50 petty-cash fund.

E. Padlocks and Combination Locks.

1. Federal Lock Specification (Padlocks)

a. Federal Lock Specification FF-P-2827A covers two sizes of a “U” shaped shackle, key operated, heavy duty commercial padlock. The padlocks covered by this specification shall be Size A, Types 1, 2, and 3, and Size B, Types 1, 2, and 3.

b. Size and Type: The size and type shall be determined by the shackle stock diameter, and the type shall be determined by keying requirements.

(1) Size A – Shackle diameter, 0.375 ± 0.020 inch (10 ± 0.051 mm) nominal
Type 1 – Individual lock (no master keying)
Type 2 – Master keyed sets
Type 3 – Keyed alike sets

(2) Size B – Shackle diameter, 0.500 ± 0.020 inch (13 ± 0.051 mm) nominal
Type 1 – Individual lock (no master keying)
Type 2 – Master keyed sets
Type 3 – Keyed alike sets

c. Description: The “U” shaped non-removable type shackle, general field service, keyed operated padlock has a body (or case) that has no projections which will cover or shroud the shackle. The padlock shall offer a high degree of protection against the various forms of corrosion and deterioration encountered in inclement environments and harsh operational conditions. The major components of a padlock shall be a body, a keyed cylinder, a heel and toe dead bolt locking mechanism and a retained “U” shaped shackle.

2. Federal Lock Specification (Combination Locks).

a. Federal Lock Specification FF-L-2740A replaced UL Group 1R requirements for GSA-approved security containers in 1991 to reduce the inherent security risks associated with conventional technology. Group 1R lock specifications were applicable for GSA-approved security containers from 1962 to 1991.

b. Currently, the Mas-Hamilton Group, Model X-07, X-08, X-09 and the Sargent & Greenleaf 2740 have received GSA approval. Model X-07 and X-08 are no longer manufactured; however they may still be used. This changeable combination lock is a self-powered microcomputer lock with a liquid crystal display. Any existing Group 1R locks on GSA "red label" containers, i.e., all containers produced after March 1991, should be replaced with the above locks when the existing locks become unserviceable.

3. UL-Rated Combination Locks. A variety of manufacturers have produced UL-rated changeable combination locks. These locks have been available for many years and continue to be installed on the various containers described above. Combination locks may be of the hand-change or key-change type. These types of locks are classified by UL as Group 1, Group 1R, or Group 2 according to the degree of protection afforded against unauthorized opening.

a. Group 1. Group 1 combination locks afford a choice of at least 1,000,000 combinations and are highly resistant to expert or professional manipulation for a period of 20 man-hours. Group 1 locks are considered suitable for use of burglary-resistant safes and chests.

b. Group 1R.

(1) Group 1R combination locks afford a choice of least 1,000,000 combinations and are highly resistant to expert manipulation. In addition to resisting unauthorized opening by expert manipulation for a period of 20 man-hours, these locks are secure against radiological attack for 20 hours, with a radioactive source not exceeding the equivalent of 10 curies of Cobalt 60 at a 30-inch distance. Group 1R locks are considered suitable for use on burglary-resistant safes and vaults. Group 1R locks were specified for GSA-approved security containers from 1962 to 1991.

(2) Locks on previously approved GSA “black label” security containers that require replacement due to age or mechanical failure should be replaced with locks meeting Federal Specification FF-L-2740A.

c. Group 2. Group 2 combination locks afford a choice of at least 1,000,000 combinations and are reasonable resistant to unauthorized openings. These combination locks are considered suitable for use on insulated safes, insulated record containers, insulated vault doors, light vault doors, and tamper-resistant doors.

F. Combinations.

Refer to DLAI 6304, Information Security Program.

G. Repairing Security Containers.

Refer to DLAI 6304, Information Security Program.

CHAPTER 9: CONTROL OF PRIVATELY-OWNED WEAPONS

A. General.

1. Privately-owned weapons and ammunition legally purchased under Federal, State, and local laws by personnel residing at DLA installations may be stored at the installation small arms storage facility or their residence; separate from DLA-owned and stored weapons. Such weapons will be stored in locked metal racks or containers. A receipt for these types of weapons will be retained in the storage facility when the weapons are in the possession of the individual owners.

2. Privately-owned weapons will not be brought onto DLA installations by personnel who do not reside at the installation. (This does not apply to Federal and local police agencies while on official duty at the installation.)

3. Specific instructions concerning the security of privately-owned weapons will be published locally and will include the requirement for initial registration of such weapons with the Chief, Security and Emergency Services.

4. Installation personnel will be notified of all provisions governing the possession, storage, and use of privately-owned weapons. Procedures will be established to ensure that all newly-assigned personnel are advised of these provisions at the time of initial orientation.

5. DLA Activities that are tenants on installations will follow host procedures.

6. For additional information refer to the message from the Secretary of Defense office dated 031913Z Dec 10, Subject: Privately Owned Weapons. In addition, all federal facilities are governed by 41 CFR § 102–74.440.

B. Developing Local Policy.

Policy and procedures may vary from installation to installation dependent upon the results of assessments and the degree of control Installation Commanders' desire. As a minimum, policy will establish requirements and procedures in the following areas.

1. Registration of firearms and unusually dangerous weapons on DLA installations. Individuals who register and store privately-owned weapons at DLA installations must comply with applicable local and State laws and DLA policy regarding weapon registration.

2. Storage of firearms and unusually dangerous weapons in housing, billeting, and any permanent or temporary living facility on-base.

3. Prohibiting transportation of firearms and unusually dangerous weapons in motor vehicles on-base.

4. Sale, purchase, and distribution of firearms or unusually dangerous weapons on-base.

5. Use of on-base lands or facilities for discharging firearms or use of unusually dangerous weapons.

6. Sharing or posting information containing lists of weapons, their owners, and location of weapons with security forces and other agencies or personnel reasonably needing access to such information.

C. Family Housing Storage.

DLA Installation Commanders may authorize the storage of privately-owned weapons in installation family housing provided the weapons are properly secured in accordance with local security and safety regulations. Privately-owned weapons will not be stored in Temporary Quarters or visitor quarters.

D. Prohibited Weapons and Ammunition.

1. Explosive weapon. Any explosive or incendiary bomb, grenade, rocket, or mine, that is designed, made, or adapted for the purpose of inflicting serious bodily injury, death, or substantial property damage, or for the principal purpose of causing such a loud report as to cause undue public alarm or terror, and includes a device designed, made, or adapted for delivery or shooting an explosive weapon.

2. Firearm. In accordance with Title 18, U.S. Code, Part 1, Chapter 44, a firearm is any device designed, made, or adapted to expel a projectile through a barrel by using the energy generated by an explosion or burning substance or any device readily convertible to that use. Firearms do not include weapons that may have, as an integral part, a folding knife blade or other characteristics of weapons such as:

a. An antique or curio firearm manufactured before 1899; or

b. A replica of an antique or curio firearm manufactured before 1899, but only if the replica does not use rim fire or center fire ammunition.

3. Machine gun. Any firearm that is capable of shooting more than two shots automatically, without manual reloading, by a single function of the trigger.

4. Short-barrel firearm. A rifle with a barrel length of less than 16 inches or a shotgun with a barrel length of less than 18 inches, or any weapon made from a shotgun or rifle if, as altered, it has an overall length of less than 26 inches.

5. Knife. Any bladed hand instrument that is capable of inflicting serious bodily injury or death by cutting, slashing, chopping or stabbing a person with the instrument. This also includes any nondescript object to conceal a bladed weapon. Prohibited bladed weapons are:

a. Knife with a blade over two and one-half inches.

b. Hand instrument designed to cut or stab another by being thrown.

c. Dagger, including but not limited to a dirk, stiletto, and poniard.

d. Bowie knife.

e. Sword.

6. Switchblade knife. Any knife that has a blade that folds, closes, or retracts into the handle or sheath and that opens automatically by pressure applied to a button or other device located on the handle

or opens or releases a blade from the handle or sheath by the force of gravity or by the application of centrifugal force. The term does not include a knife that has a spring, detent, or other mechanism designed to create a bias toward closure and that requires exertion applied to the blade by hand, wrist, or arm to overcome the bias toward closure and open the knife.

7. Knuckles. Any instrument that consists of finger rings or guards made of a hard substance and that is designed, made, or adapted for the purpose of inflicting serious bodily injury or death by striking a person with a fist enclosed in the knuckles.

8. Armor-piercing ammunition. Handgun ammunition that is designed primarily for the purpose of penetrating metal or body armor and principally used in pistols and revolvers.

9. Chemical dispensing device. A device, other than a small chemical dispenser sold commercially for personal protection, that is designed, made, or adapted for the purpose of dispensing a substance capable of causing an adverse psychological or physiological effect on a human being.

10. Zip gun. A device or combination of devices that was not originally a firearm and is adapted to expel a projectile through a smooth-bore or rifled-bore barrel by using the energy generated by an explosion or burning substance.

11. Club. An instrument that is specially designed, made, or adapted for the purpose of inflicting serious bodily injury or death by striking a person with the instrument, and includes but is not limited to the following:

a. Blackjack;

b. Nightstick;

c. Mace;

d. Tomahawk;

e. Bow and Arrow.

12. Other Dangerous Weapons. Any other instrument designed, made, or adapted to propel a projectile with sufficient force to inflict serious bodily injury or death by piercing or blunt trauma.

CHAPTER 10: DESIGNATION AND PROTECTION OF SECURE AREAS

A. General.

1. Different degrees of security protection are required for DLA's operations. The variance in security protection results from the nature and purpose of mission requirement, the information or material contained in the area, and the identified risks to the operations or the material. Designation and establishment of secure areas are the responsibilities of DLA PLFA Commanders/Directors. To assist in this designation process, DLA uses the terms, in descending security sensitivity, Restricted Area and Controlled Area.

2. *The Internal Security Act of 1950* (50 U.S.C. 797), Section 21, provides for military Commanders of DoD installations to promulgate orders and regulations to ensure the security of DoD personnel, property, and equipment. DoD Instruction 5200.8, *Security of DoD Installations and Resources and the Physical Security Review Board (PSRB),* identifies DoD Commanders as authorized personnel to promulgate installation security regulations and orders. DoD Directive 5105.22, *Defense Logistics Agency*, gives the Director, DLA, the authority to promulgate security orders and regulations. This manual and local directives identify the special entry conditions and security requirements of the activity.

3. Secure areas will be designated in writing and posted with warning signs in conspicuous places such as entrances and approaches to these areas and on perimeter fences or barriers of the areas. The designations Restricted Area or Controlled Area are the only descriptive terms that will be indicated on the signs.

4. For restricted and controlled areas, written operating procedures must be developed by owner/user personnel covering, as a minimum, the following areas.

a. Entry/exit control procedures.

b. Bomb threat procedures.

c. Other emergency evacuation procedures for fires, etc.

d. Owner/user personnel training requirements.

e. Visitor control procedures.

5. The designation or non-designation of secure areas will not be based on existing physical security measures or the lack thereof.

B. Considerations.

There are other important considerations concerning secure areas and their lines of division. These considerations include the following:

1. A survey and analysis of the installation/facility, its missions, and its security interests to determine immediate and anticipated needs that require protection. Anticipated needs are determined from plans for the future.

2. The size and nature of the security interest being protected. Safes may provide adequate protection for classified documents and small items; however, large items may have to be placed within guarded enclosures.

3. Some security interests are more sensitive to compromise than others. Brief observation or a simple act by an untrained person may constitute a compromise in some cases. In others, detailed study and planned action by an expert may be required.

4. All security interests should be evaluated according to their importance. This may be indicated by a security classification such as confidential, secret, or top secret.

5. Parking areas for POVs are established outside of restricted areas. Vehicle entrances must be kept at a minimum for safe and efficient control.

6. Physical protective measures (such as fences, gates, and window bars) must be installed. Additional protective and construction requirements may be found in applicable DoD Directives (see Glossary of References).

C. Restricted Areas.

Defined as an area in which there are special restrictive measures employed to prevent or minimize incursions and/or interference, where special security measures are employed to prevent unauthorized entry. Restricted areas must be authorized in writing by the PLFA Commander/Director, properly posted, and shall employ physical security measures. Visitors to a restricted area and uncleared personnel must be escorted by personnel assigned to the area and all classified and sensitive information must be protected from observation, disclosure, or removal.

1. Restricted Areas:

a. Open storage areas authorized to store classified information

b. Data processing centers processing classified information including server rooms, tape libraries, computer rooms, and removable disks containing backup data.

c. Communication centers.

d. Cryptographic areas.

e. Storage areas for "R" coded material.

f. Storage areas for "Q" coded material (non-bulk).

g. Armory/AA&E storage facilities

h. Storage areas for “9” coded material

i. Storage areas for “O” coded material

j. Storage areas for ODS material

2. Security Procedures. The following security procedures apply to all Restricted Areas unless otherwise stated.

a. The area will be designated a Restricted Area and signs will be posted on the outside doors and the perimeter of the area.

b. Owner/users of the Restricted Area are responsible for designating in writing a Restricted Area monitor. The Chief, Security and Emergency Services/Chief, Security Services, is responsible for training all monitors.

c. Restricted Area Monitors will maintain a continuity book for their respective area that will contain, at a minimum, the following:

(1) Designation of Restricted Area letter

(2) Restricted Area Monitor appointment letter

(3) Three physical security inspections of Restricted Area, including initial, last Higher Headquarters assessment, and last self-assessment.

(4) Visitor Control logs maintained in accordance with Records Management procedures.

(5) At least one year of alarm test records

d. Access lists and security badges will be used to control access to the area. Only those individuals identified on the access list will be allowed unescorted access to the area.

e. Personnel designated to control entry will use the DLA Form 584 to record movement of personnel in and out of the secure area.

f. Visitors will be escorted at all times in accordance with local policy.

g. Combination(s) and/or keys to the entrance door will be safeguarded in accordance with this manual. Combinations will be changed at least once a year or when any personnel having access to the combination are reassigned, separated, or no longer have a need for this information.

h. At the close of business, designated operating personnel will perform a security check prior to departure. Local procedures will be established which will document daily checks and at a minimum will verify that all windows, doors, equipment and property are properly secured, and that the alarm system is functional.

i. During non-duty hours the area will be protected by an ESS and will be checked by a police patrol at intervals not to exceed four hours. Outside storage areas storing classified material will be checked by a police patrol at intervals not to exceed two hours.

j. Additional local procedures (i.e.,SOPs) for all Restricted Areas will prescribe in writing security measures for inspections of items moving in and out of the area, opening and closing of the door, trash removal, restrictions regarding briefcases, purses, lunch boxes, etc., searches, and visitor control. For prohibited items, refer to the DoD Information Security Regulation, DoD 5200.1-R (http://www.dtic.mil/whs/directives/corres/pdf/520001r.pdf).

k. Open Storage areas must additionally meet the requirements detailed in Section E, below and Appendix E, Open Storage Inspection Checklist.

l. The following procedures apply only to material storage areas designated as Restricted Areas.

(1) Positions for employees' assigned duty in the areas storing "Q" and "R" coded material will be in accordance with DLAR 4145.11, IV, para D 1

(2) POVs are not allowed to park within 50-feet of entrance/exit doors of storage areas.

(3) Material to be shipped will be loaded on carriers directly from the Restricted Area and will not be pre-staged outside the secure area to await loading.

(4) All unexplained shortages, suspected pilferage, or compromise will be reported immediately to the Chief, Security and Emergency Services/Chief, Security Services.

(5) The Restricted Area monitor will conduct annual inspections of secure storage areas using the checklist provided by the installation Physical Security Specialist to ensure adequacy of physical security measures and compliance with security policies. Reports of findings resulting from these inspections will be submitted to the Installation/Facility Commander/Director through the Director of the affected area and DLA Installation Support, Security and Emergency Services.

(6) The Installation/Facility Physical Security Specialist will review the storage locations of all controlled items at least triennially. During off years, the Restricted Area monitor is responsible for conducting self inspections. The Restricted Area monitor will review the storage locations of all controlled items at least monthly to ensure the items are properly stored and protected.

(7) In areas storing "R" coded material, a DLA Access Badge/CAC may be coded for each person authorized entry into the vault. The entry control personnel will issue the exchange badge after verifying that the employee's name is on the access list. The DLA Form 584 will be used to record movement of personnel in and out of the vault.

D. Controlled Areas.

This area is designated in writing by the Installation Commander/Director, wherein sensitive resources, information or operations occur and requires limited and controlled access. Admittance to a controlled area is limited to persons who have official business within the area

1. Controlled Areas.

a. Fund handling areas (more than $25,000).

b. Central mail room.

c. IT centers processing unclassified information to include server rooms, tape libraries and computer rooms.

d. Security Operations Center.

e. ESS Alarm Rooms

f. DLA Energy fuel storage facilities.

g. Storage areas for pilferable items. For more information refer to DLAR 4145.11.

h. Storage areas for "Q" coded material (bulk).

i. Storage areas for hazardous material.

j. Storage areas for medical supplies.

2. Security Procedures. The following security procedures apply to all Controlled Areas unless otherwise stated.

a. The area will be designated in writing as a Controlled Area and signs will be posted on the outside doors and perimeter of the area.

b. Owner/users of the Controlled Area are responsible for designating in writing a Controlled Area monitor. The Chief, Security and Emergency Services/Chief, Security Services, is responsible for training all monitors.

c. Controlled Area monitors will maintain a continuity book for their respective area that will contain, at a minimum, the following:

(1) Designation of Controlled Area letter

(2) Controlled Area Monitor appointment letter

(3) Three physical security inspections of Controlled Area, including initial, last higher HQ assessment, and last self-assessment.

(4) Visitor control logs maintained in accordance with Records Management procedures.

(5) At least one year of alarm test records (if Area alarmed)

d. The Controlled Area will have only one active personnel entrance. During normal duty hours the entrance will be locked and entry will be controlled by designated on-duty personnel. Other entrances and exits will be secured and exit doors will be equipped with panic bar-type locking devices.

e. Access lists and security badges will be used to control access into the area. Only those individuals identified on the access list will be authorized unescorted access to the area.

f. Personnel designated to control entry will use the DLA Form 584 to record movement of personnel in and out of the secure area.

g. Visitors will be escorted at all times.

h. Keys to the area will be controlled in accordance with Chapter 9 of this manual.

i. Local procedures will prescribe security controls for the movement of items and personnel in and out of the secure area and for inspections of packages.

j. At the close of business, designated operating personnel will utilize SF 701 to perform a security check prior to departure. In addition, SF 701 can be amended and used to document daily checks of window(s), door(s), equipment, and property to ensure that they are properly secured and the alarm is set. If SF 701 is not amended and used for daily checks, local procedures will be established which will document the above.

k. During off duty hours the area will be protected by the alarm system and will be checked by a security patrol at intervals not to exceed eight hours.

l. The following procedures apply only to material storage areas designated as Controlled Areas.

(1) POVs are not allowed to park within 50-feet of entrance/exit doors of storage areas.

(2) Positions for employees' assigned duty in the areas storing "Q" coded material will be in accordance with DLAR 4145.11, IV, para D 1.

(3) Material removed from the secure area for shipment will be loaded on carriers as soon as possible. Items received at a consolidated receiving area will be transferred to the appropriate secure area as soon as possible. A cage or container will be available at designated staging areas for temporary storage of items that are awaiting shipment or transfer.

(4) All unexplained shortages or suspected pilferage will be reported immediately to the Chief, Security and Emergency Services/Chief, Security Services.

(5) The Controlled Area monitor will conduct annual inspections of secure storage areas using the checklist provided by the local Physical Security Specialist to ensure adequacy of physical security measures and compliance with security policies. Reports of findings resulting from these inspections will be submitted to the PLFA Commander through the Director of the affected area and DLA Installation Support, Security and Emergency Services.

(6) The PLFA Physical Security Specialist will review the storage locations of all controlled items at least triennially. During off years, the Controlled Area monitor is responsible for conducting self inspections. The Controlled Area monitor will review the storage locations of all controlled items at least monthly to ensure the items are properly stored and protected.

E. Open Storage Area Policy

1. In accordance with DoD 5200.08-R, Physical Security Program, and DoD 5200.1-R, Information Security Program, the following procedures shall be followed for open storage areas at DLA locations.

2. As outlined under DoD 5200.1-R, Appendix 7, secure rooms used for open storage must adhere to prescribed physical security standards. In each instance where open storage approval is sought, the requestor shall provide the Information Security Specialist with the regulatory requirement(s) to ensure there is a valid need for open storage. Once validated, the local Physical Security Specialist and Information Security Specialist shall conduct a joint inspection of the requested open storage area(s) to verify and document adherence to DoD standards using the DLA Open Storage Checklist (Appendix E) for each open storage area request.

3. The DLA Open Storage Approval form (DL1922) shall be accompanied by the completed Open Storage Inspection Checklist to provide background documentation. If approved, a signed open storage approval letter by DLA Intelligence (DI) and DLA Installation Support, Security and Emergency Services (DS-S) will then be provided to the requestor. If either DI or DS-S disapproves the request, the open storage approval form will be sent back to the requestor with the necessary actions and recommendations to be taken in order to receive approval. In situations where DLA is a tenant, the host grants open storage approval and DLA tenants shall forward a copy of the open storage approval form to DLA Installation Support, Security and Emergency Services. Approvals are valid for a period of three years from the date they are signed and shall be kept on file and made available to inspectors. Note that any changes or modifications made to physical structures or addition/deletion of any equipment without the authority of the Staff Director, DLA Installation Support, Security and Emergency Services will cause suspension of open storage approval.

4. To assist with inspections and audits, the following documents and records shall be maintained for each open storage area:

a. Post the signed open storage approval form within the open storage area;

b. Detailed floor plans/diagrams of open storage area including doors/windows and location of alarm devices;

c. Security Plan including entry/exit procedure, emergency evacuation plan, and power/alarm system loss procedures;

d. Local procedures to document end of day checks – verify all windows, doors, equipment, and property are properly secured, and that alarm system is activated via SF 701 (Activity Security Checklist) and SF 702 (Security Container Check Sheet);

e. Additional local procedures for: inspection of items moving in and out of the area, trash removal, and searches and visitor control;

f. Access control list for employees with access to open storage area;

g. DLA Form 584, recording movement in and out of security area by visitors;

h. Combination change schedule in accordance with DLAI 6304;

i. Log for recording quarterly alarm tests;

j. Post signs prohibiting personal electronic devices.

F. Designation of Resource Levels and Levels of Security

1. General.

a. PLFA Commanders/Directors are responsible for the protection of resources located on their installations/facilities. The Resource Level (RL) System will be utilized to identify what resource level will be assigned and the additional level of security required at each RL. RL's will be identified as RL1, RL2 and RL3. The RL system will also apply to resources assigned to tenant organizations on DLA Installations. Additionally, when an Installation/Facility has an IDS that protects many alarmed areas,

each area must be clearly distinguishable from the other to facilitate a priority response. The RL will allow the PLFA Commander/Director to establish an Alarm Priority Response List (APRL) to ensure immediate armed response to higher priority resources. Responses to RL1 resources will have priority over RL2 and RL3 resources. Responses to RL 2 resources will have priority over RL3 resources.

Note: DLA tenant activities will work with the Host installation IAW written ISSAs, MOUs or MOAs to ensure RL guidance intent is met.

b. The Installation/Facility Force Protection Working Group (FPWG) will ensure the owner/user of the resource coordinates on the RL assigned to their resource. To determine the priority of resources assigned within a RL, the criticality assessment of each resource will be used. The FPWG will accumulate the data, create an APRL and forward its recommendation to the Installation's Security Executive Committee (ISEC). Upon the ISEC review and approval, the information will be an annex to the installation physical security plan and only be provided to organizations that have a need to know. The following paragraphs will provide definitions and examples of resources that will be categorized as RL 1, 2 or 3. RL 3 will be assigned to resources that do not meet the definitions of RL 1 and 2.

2. Resource Level 1 (RL1).

a. RL1 is assigned to resources located on DLA installations/facilities that the loss, theft, destruction, misuse, sabotage or compromise would cause grave damage to the DoD war-fighting capability and/or national security.

b. Examples

(1) Selected Critical Command, Control and Communications (C3) facilities, systems, or equipment.

(2) Expensive, few in numbers, or one of a kind systems.

(3) Intelligence-gathering systems critical to US operational capability.

(4) Vital computer facilities and equipment.

(5) Facilities storing any number of Category I, II, III, or IV Sensitive Conventional AA&E.

3. Level of Security for RL1.

a. Security measures employed must result in significant deterrence against hostile acts. Security will ensure a significant probability of detecting and intercepting hostile intentions. The following security measures will be employed in addition to those mentioned in C para 2 a-k above.

b. Restrict entry to the areas.

c. Expand the security of the area with defense-in-depth and active patrolling.

d. Provide IDS and surveillance at the perimeter (Position armed security officers at the area when IDS not operational or installed).

e. Provide police officers to respond to alarm activations.

4. Resource Level 2 (RL2).

a. RL2 is assigned to resources located on DLA installations/facilities that the loss, theft, destruction, issue, sabotage or compromise of would cause serious damage to the DoD war-fighting capability and/or national security.

b. Examples:

(1) Selected Command, Control, and Communications (C3) facilities, systems, and equipment.

(2) Intelligence-gathering systems not critical to US operational capability.

5. Level of Security for RL2.

a. Security measures employed must result in a reasonable degree of deterrence against hostile acts. Security will ensure the capability to impede a hostile force and limit damage to resources. The following security measures will be employed in addition to those mentioned in C para 2 a-k above.

b. Control entry to areas.

c. Provide IDS and surveillance at the perimeter.

d. Provide police officers to response to alarm activations.

6. Resource Level 3 (RL3).

a. RL3 is assigned to resources located on DLA installation/facilities that the loss, theft, destruction, misuse, sabotage or compromise of would cause damage to national security and/or adversely affect the operation capability of DLA and its tenants. RL3 resources are contained in areas with owner/users being primarily responsible for security. Response is provided by DLA Police.

b. Examples:

(1) Mission essential communications facilities and computer centers.

(2) Power plants and environmental control systems critical to operational capability.

(3) Fuels and Liquid Oxygen Storage Areas.

(4) Warehouses storing aircraft or weapons systems spare parts.

(5) Medical logistics vaults.

7. Level of Security for RL3.

a. Security measures employed must reduce the opportunity for theft or damage to resources. The following security measures will be employed in addition to those mentioned in D para 2 a-m above.

b. Owner/user will:

(1) Implement entry and circulation control procedures in controlled areas.

(2) Identify assigned mission essential resources.

(3) Ensure proper training of assigned personnel.

(4) Provide physical protection and conduct security inspections in accordance with all applicable directives.

c. Installation/Facility Chief, Security and Emergency Services/Chief, Security Services will:

(1) Conduct random patrols in areas.

(2) Monitor IDS where required.

(3) Provide police response to alarm activations, when required.

(4) Provide technical guidance and advice to owner/user.

(5) Conduct physical security surveys in accordance with all applicable directives.

G. Warning Signs.

1. General. Installation Boundary, Restricted Area, and Controlled Area warning signs will be fabricated of metal with black lettering on a white background, except that words shown in all capital letters will be red. Existing signs need not be replaced provided the signs are in good repair, the lettering is legible, and the wording conforms to the above requirements. Interior signs may be fabricated of wood, metal, plastic, or cardboard.

2. Installation Boundary Signs.

a. Design and wording will be as follows:

WARNING
(Enter name of Installation)
It is unlawful to enter this installation without permission of the Installation Commander.
Section 21 of the Internal Security Act of 1950, 50 USC 797.
While in this installation, all personnel and the property under their control are subject to search.

b. Signs will be posted at all installation entrances and approaches. Additional signs will be posted along the boundaries of such areas not to exceed 500- feet between each sign.

3. Restricted Area Signs.

a. Design and wording will be as follows:

WARNING
Restricted Area

It is unlawful to enter this area without permission of the Installation Commander.
Section 21 of the Internal Security Act of 1950, 50 USC 797.
While in this area all personnel and the property under their control are subject to search.

b. Signs will be posted at all Restricted Area entrances and approaches. Additional signs will be posted along the boundaries of such areas not to exceed 500- feet between each sign.

4. Controlled Area Signs.

a. Design and wording will be as follows:

WARNING
Controlled Area
It is unlawful to enter this area without permission of the Installation Commander.
Section 21 of the Internal Security Act of 1950, 50 USC 797.
While in this area, all personnel and the property under their control are subject to search.

b. Placement will be as prescribed for Restricted Area signs.

5. Sign Sizes.

a. Installation Boundary - 2-feet X 1-foot.

b. Personnel and Vehicle Entry Points - 4-feet X 2-feet.

c. Building, area and interior personnel entry points such as cashier cages, firearms facilities, etc., 2-feet X 1-foot.

d. For administrative areas where the 2-feet X 1-foot sign would detract from the aesthetic value of the area, signs may be reduced in size if proper wording and legibility is maintained.

CHAPTER 11: GOVERNMENT FUNDS PROTECTION

A. Applicability.

1. The standards and procedures in this section apply to all appropriated, nonappropriated, and other Government funds or negotiable instruments under DLA control.

2. Those businesses located on DLA activities will comply with these standards and procedures.

3. Army and Air Force Exchange Service (AAFES) facilities will be guided by the protection requirements in AAFES manuals provided those requirements provide protection equal to or greater than the standards prescribed herein.

4. Commissary sales stores will be secured in accordance with applicable commissary operating manuals provided those requirements provide protection equal to or greater than the standards prescribed herein.

5. Imprest funds will be controlled and secured in accordance with the procedures contained in this section; unless otherwise indicated. Imprest funds will be inspected at least annually by security personnel for compliance with local procedures and this manual.

6. Class VI (package beverage) stores will be secured in accordance with applicable operating manuals provided those requirements provide protection equal to or greater than the standards prescribed herein. Storage and sales areas will be designated and posted as Controlled Areas. Entrances and exits to sales and storage areas will be protected by an intrusion detection system during nonoperational periods.

7. Where a contractual relationship exists (as with an exchange concessionaire), security of funds will be a part of the contract.

B. General Guidelines:

1. Controlled Area Designation for Funds Facilities. All funds facilities handling or storing $25,000 or more will be designated as Controlled Areas. The decision to designate other funds facilities as Controlled Areas rests with the PLFA Commander/Director, but is discouraged.

2. Protecting High Cash Value Resources. Protect these resources according to their dollar value as prescribed by this chapter. Do not count these items when determining the total amount of funds for storage purposes.

a. United States Postal Services postage stamp stocks.

b. Blank money orders and Government pay checks.

c. Negotiable instruments marked payable to the United States Treasury, stamped For Deposit Only, or made payable to an Accounting and Finance Office or a nonappropriated fund instrumentality but not endorsed.

3. Funds will not be stored in any container that is being used to store classified information or material.

4. Except for central depositories, any fund container on casters or one that weighs less than 500 pounds and is not protected by an IDS system or not located inside a vault will be secured to the premises. It may be secured by bolts or heavy metal straps or, if it is intended to remain part of the structure, it may be secured by imbedding it in concrete.

C. Responsibilities of the Funds Activity Custodian.

Fund handling activities will designate a fund custodian in writing to the installation Chief, Security and Emergency Services. The custodian is responsible for the following.

1. Protecting Funds. Ensure funds are protected as prescribed by this manual and according to local procedures.

2. Operating Instructions. Publish a local operating instruction, outlining procedures for the following, as a minimum:

a. Use DLA Form 1886, *Robbery Checklist* and actions to take in the event of a robbery.

b. Steps to reduce cash on hand.

c. Control of alarm systems key boxes if applicable.

d. Training procedures.

e Bomb threat procedures.

f. Funds escort procedures.

g. Controlled area entry and escort procedures.

h. Emergency entry and egress procedures.

3. Storage Approval. Obtain Installation Chief, Security and Emergency Services approval for funds storage limits.

D. Funds Escort Procedures.

1. Escorts will be furnished by either the fund activity or the security force. Contract armored car service may be used.

2. Escorts for fund amounts less than $10,000 may be armed or unarmed depending upon local conditions. The DLA PLFA Site Director's decision allowing armed escorts must be based on providing adequate protection against the local criminal threat.

3. Escorts for fund amounts of $10,000 or more will be armed.

4. When personnel are armed for the purpose of escorting funds, coordination will be made with local jurisdictions concerning the carrying of weapons off the DLA Activity and the provisions of DLA Instruction 4310, *Carrying of Firearms and Use of Force*, apply.

5. When funds are escorted regularly between a fund activity and a protected facility on the activity, the routes between the two points and times of departure will be varied. Personnel assigned as escorts will not carry funds.

6. During a security force escort, constant radio contact will be maintained between the security force escort and security operations center.

7. Escorts assigned from the fund activity will call the security force immediately prior to departure and give the time and place of departure, route of travel, destination, and estimated time of arrival. The security force will be notified upon termination of the escort.

8. Movements of funds off the activity will be closely coordinated with the local police.

9. Escorts will obey traffic regulations and all instructions of any local police escorts as long as they do not violate Federal law or lessen the protection of funds. Escorts will not use sirens or red lights except in emergencies.

10. Fund escort requirements for DLA Activities tenant on military installations will be in accordance with the criteria established by the host.

11. Transporting Funds. Escorted funds will not be transported in any vehicle operated by or carrying security forces personnel.

12. Security Forces Escorts. Security forces personnel will occupy a trail vehicle during all funds escorts.

13. Commissaries, AAFES facilities, on-base banks and non-appropriated funds facilities are encouraged to contract escort facilities. If contractor services are not available or the Security Manager determines the threat level is such that contractor services are impractical, the Security Manager will determine if security forces personnel will perform escorts for non-government funds.

E. Funds Storage Limits During Non-Operating Hours.

1. Funds facilities storing less than $10,000 do so in accordance with local installation security plan or installation security instruction guidelines.

2. Because they provide adequate forced entry protection, either a GSA-Approved Class 5 security container or an UL-rated burglary resistant safe (see Chapter 10) will be utilized to safeguard funds over $10,000. Based upon local vulnerabilities, consider installation of a panic or holdup alarm. The cost of any additional security systems should be compared with the amount of cash being safeguarded.

3. For than $10,000 but less than $50,000, each container/room used to store this amount must be alarmed.

4. Not more than $50,000 will be stored in any individual fund container unless stored inside an alarmed vault.

F. Central Repositories.

The use of a central repository under the supervision of security forces personnel is not authorized.

G. Storing Funds After Duty Hours.

Facilities subject to this manual follow these guidelines after duty hours and at cashier cages during duty hours.

1. Procedures. Keep a packet of money (including foreign currency where applicable) designated as separate from the rest of the funds. Place at least five $20 bills in the packet. Keep the bills with operating funds, but do not distribute them unless a robbery occurs at which time the bills will be included with the stolen money.

2. Recording Serial Numbers. Record the serial numbers and series year of each bill. Keep the recorded information in a separate container from the funds.

H. Use of ESS.

An effective ESS is a prime deterrent in preventing the loss of funds by theft. The following funds activities must have their funds storage areas protected by ESS.

1. Accounting and Finance Offices.

2. Facilities Storing $10,000 or More.

3. Other Funds Facilities as Required Locally.

I. Robbery Prevention and Planning.

1. A written plan describing actions to be taken in case of a robbery will be prepared for each DLA fund handling activity. A plan is also required for each non-DLA fund handling activity located on a DLA Installation. For DLA Installations, a single plan may be prepared with a separate annex for each fund activity identifying procedures unique to that activity. Plans will include the following:

a. Actions to be taken by fund handling activity employees.

b. Actions to be taken by security force officers.

c. Actions to be taken by the supporting law enforcement agency or agencies.

d. Agencies and officials to be notified and the individual, by position, responsible for the notification.

e. All required reports.

2. Robbery Prevention Plans will be coordinated with all local law enforcement agencies. DLA fund handling activities tenant in non-DLA buildings, or on military installations, will coordinate their plan with the host. Liaison with outside agencies will be conducted together with the host.

3. Robbery Prevention Plans for activities maintaining more than $10,000 during operating hours will be tested by the Office of Security and Emergency Services at least annually.

4. All fund handling personnel will receive initial and annual anti-robbery training from the installation Office of Security and Emergency Services.

5. The following prevention measures should be considered in Robbery Prevention planning:

a. Instruct employees to carefully observe persons loitering in or near the activity.

b. Encourage employees to challenge unidentified personnel.

c. Keep the amount of cash in cashier cages at a minimum level.

d. Require employees to secure all funds from their immediate work area prior to their departure.

e. Avoid establishing unnecessary operating routines.

f. Upon closing at night, ensure the safe or vault and all doors and other points of access to the activity are locked.

6. Employee Conduct During and After a Robbery. The following actions should be taken by employees during and after a robbery:

a. Avoid actions that might increase danger to yourself or others.

b. Activate the robbery alarm system if it appears that such activation can be accomplished safely.

c. Observe the robber's physical features; voice, accent, mannerism, dress, the kind of weapon he has, and any other characteristics that would be useful for identification purposes.

d. If the robber leaves evidence (such as a note), try to put it aside and out of sight if it appears that this can be done safely. Retain the evidence, do not handle it unnecessarily, and give it to the security police when they arrive.

e. Refrain from touching, and assist in preventing others from touching articles or places the robber may have touched or evidence he may have left, to preserve fingerprints of the robber.

f. Give the robber no more money than the amount he demands and include "bait" money in the amount given ("bait money" consists of a serially recorded packet of paper money inconspicuously banded or clipped for identification purposes).

g. If it can be done safely, observe the direction of the robber's escape and the description and license plate number of the vehicle used, if any.

h. Telephone the security office or inform a designated officer or other employee who has this responsibility that a robbery has been committed. Give the security force dispatcher all available information; i.e., your location, description of the robbers and the vehicle, and the escape route.

i. If the robber leaves before the police arrive, assure that a designated officer or other employee waits outside the office to inform the security police.

j. Attempt to determine the names and addresses of persons who witnessed the robbery or the escape and request them to record their observations or to assist a designated officer or other employee to record their observations.

k. Refrain from discussing the details of the robbery with others before recording the observations. This will assist in keeping the memory clear of distractions.

l. When safe to do so, document pertinent information on DLA Form 1886.

J. Security Checks.

1. Security managers will establish local procedures for daily checks of fund handling activities by security force personnel.

2. In the event of alarm malfunction, the owner/user is responsible for responding to assume responsibility of the area, according to local procedures. Security checks will be performed at least once every 2 hours during nonoperational hours.

3. All security checks will be annotated and the record maintained for 30 days per GRS 18, item 18b but does not include records of security checks that reflect a security violation.

CHAPTER 12: ARMS, AMMUNITION, AND EXPLOSIVES (AA&E)

A. General.

In accordance with DoD 5100.76-M , this Manual prescribes minimum standards and criteria for the physical security of DoD sensitive conventional AA&E, including non-nuclear missiles and rockets, in the custody of any DLA component or DLA contractor. DLA components may impose additional protective measures above those prescribed herein where warranted. However, such measures shall not violate or conflict with DoD 6055.9-STD, "DoD Ammunition and Explosives Safety Standards." DLA operational requirements and the need to moderate manpower and material costs dictate prudence in achieving a balance between security and acceptable degrees of risk.

B. Policy.

1. AA&E facilities shall be consolidated to the maximum extent possible consistent with operational, safety, and mission requirements to reduce protection costs.

2. AA&E facilities to be built at land-based facilities shall be constructed in accordance with the security structural requirements of DoD 5100.76-M, and existing facilities shall be upgraded to also meet the requirements. Such facilities shall be prioritized for security upgrade as follows:

a. Facilities storing Category I items.

b. Facilities storing Category II items.

c. Facilities storing Category III and IV items.

3. Personnel assigned custody, maintenance, disposal, or security responsibilities for AA&E on DoD installations shall be subject to one of the following investigations as set forth in DoD 5200.2-R:

a. Military Personnel: National Agency Check, Local Agency Check, Credit Check (NACLC).

b. DoD Civilian Personnel: National Agency Check with Written Inquiries (NACI).

c. Contractor Personnel: NACLC

4. Prior to assumption of such duties (and at least annually thereafter), personnel responsible for the accountability of AA&E shall be made aware of the importance of accurate receipt, dispatch, and inventory records. Adherence to the requirement for scheduled inventories will be stressed, as well as procedures for processing inventory adjustment gains and losses as prescribed in DoD 4140.1-R

5. Installation physical security plans required for DLA components shall address the protection of AA&E. The host installation/activity shall assume responsibility for coordinating tenant AA&E protective measures.

6. Where an IDS is installed in a facility outside a military installation, arrangements shall be made to connect to local police or commercial monitoring companies from which immediate response to activated alarms can be directed. Response agreements/requirements shall be documented in applicable contracts and/or memorandums.

7. A daily log shall be maintained of all alarms received. Logs shall be maintained for a minimum of 90 days and shall be reviewed to identify and correct IDS reliability problems. The log shall reflect the following:

a. Nature of the alarm (nuisance, system failure, illegal entry).

b. Date, time, and location of alarm.

c. Action taken in response to the alarm.

8. Systems shall be tested quarterly to ensure the proper functioning of the alarm sensors. For bulk storage areas (depots, weapon stations, etc.), such checks may be performed every six months. A log shall be maintained documenting such tests and shall be kept for one year.

C. Key and Lock Control.

1. Keys to AA&E storage areas, buildings, rooms, racks, containers, and IDS shall be maintained separately from other keys. They shall be accessible only to those individuals whose official duties require access to them. A current roster of personnel authorized key access shall be maintained and kept from public view.

2. The number of keys shall be held to the absolute minimum. Master keying of locks and the use of a master key system is prohibited for AA&E exterior access doors.

3. Keys shall not be left unsecured or unattended at any time. In the event of lost, stolen, or misplaced keys, the affected locks or lock cores shall be replaced immediately.

4. When not attended or in use, operational keys to Category I and II AA&E shall be secured in GSA-approved Class 5 security containers or Class 5 weapons storage containers. Keys to Category III and IV AA&E may be stored in containers of at least 12-gauge steel (or material of equivalent strength) secured with a GSA-approved built-in three position changeable combination lock, a built-in combination lock meeting UL Standard 768 Group I, or a GSA-approved key-operated security padlock. Existing containers other than 12-gauge may continue to be used. Reserve or replacement locks, cores, and keys will also be secured as prescribed above. Keys will not be removed from DLA-controlled space (off installation) except for operational necessity. Installation Commanders/Directors storing/securing AA&E, or their designees, shall appoint in writing AA&E lock and key custodians. Key custodians shall not be unit armorers or other persons responsible for the AA&E storage facilities. Key control registers shall be maintained to reflect continuous key accountability and contain the following information:

a. Name and signature of individuals receiving keys.

b. Date and hour of issuance.

c. Key serial numbers or other identifying information.

d. Signature of individuals issuing keys.

e. Keys return date and hour.

f. Name and signature of individual receiving returned keys.

5. Completed key control registers shall be retained in activity files for a minimum of one year and then disposed of in accordance with local guidance.

6. Inventories of keys and locks shall be conducted semiannually. Inventory records shall be destroyed 6 months after turn-in of key, lock, combination change, etc. and then disposed of in accordance with local guidance.

D. Entry Control.

1. Strict personnel and vehicular access control shall be established for areas storing AA&E. Persons authorized unaccompanied access will be authorized in writing by the head of the AA&E activity. Visitors will be escorted at all times. Access to such areas for all personnel shall be recorded (manually or electronically). The records of access shall be retained for one year and disposed of in accordance with local guidance.

2. Vehicles and personnel shall be subject to random inspections upon entry to and exit from AA&E areas.

3. Privately owned vehicles shall be prohibited from AA&E areas.

E. AA&E Waiver Process.

DLA components may deviate from standards prescribed in this manual with approval. Additional information may be found in Chapter 16, Waivers, Variances, and Exceptions.

F. Category I, II, & III Missiles, Rockets, Ammunition and Explosives.

1. Category I, II, and III Missiles and Rockets, and all categories of Ammunition and Explosives shall be stored in fixed structure prescribed in DoD 6055.9-STD. If operational necessity dictates, Category III and IV A&E may also be stored in pre-engineered explosives magazines as specified in Naval Facilities Engineering Service Center Technical Data Sheet 82-12, dated May 1985, or a similarly constructed Component-prescribed structure.

2. Category I, II, and III Missiles and Rockets, and all categories of Ammunition and Explosives shall be stored in original containers, banded, and sealed to reflect the integrity of the contents. Generally, containers weighing less than 500 pounds shall be fastened to the structure, or fastened together in groups, which have a total weight exceeding 500 pounds with bolts or chains secured with padlocks meeting Commercial Item Description (CID) A-A-1927. Where such fastenings hinder operational requirements, the facility manager may waive this requirement. Locks assigned National Stock Number (NSN) 5340-00-158-3805, NSN 5340-00-158-3807, NSN 5340-01-408-8434, or NSN 5340-01-269-9345, all meet this CID.

3. Each magazine and/or structure storing Category I and II Missiles and Rockets and Category I and II A&E shall be equipped with an IDS unless the areas where they are located are continuously manned or under constant surveillance in such a manner that unauthorized entry into and around the storage structures can be detected. In addition to the IDS, a supervised armed (where allowed by local jurisdiction) security force individual(s) shall check all alarmed structures in the areas daily during non-duty hours. Structures containing Category III Missiles and Rockets and Category III and IV A&E do not

require IDS. However, they do require security force checks daily during non-duty hours. If these structures are equipped with IDS, no daily security force check during non-duty hours is required.

4. Storage structures shall be secured with high security padlocks and hasps.

5. The perimeter of Category I and II storage areas shall be fenced as follows:

a. Fence fabric shall be chain link (galvanized, aluminized, or plastic coated woven steel) 2-inch square mesh 9-gauge diameter wire, including coating. In Europe, fencing may be North Atlantic Treaty Organization (NATO) Standard Design Fencing (2.5-3 mm gauge, 76mm grid opening, 2-meter height, and 3.76-meter post separation).

b. The minimum height of the fence fabric shall be 6 feet (excluding top guard/outrigger).

c. Clear zones shall be established and shall extend a minimum of 12 feet on the outside and 30 feet on the inside (available real estate permitting).

d. The perimeter fence shall have a minimum number of vehicular and pedestrian gates, consistent with operational requirements. Unless continuously guarded, gates shall be secured with approved locking devices. Hinge pins shall be welded (or otherwise secured).

e. Drainage structures and water passages penetrating the fence having a cross-sectional area greater than 96 square inches, and a dimension greater than 6 inches shall be barred.

f. If the installation housing the Category I and II storage areas has adequate perimeter fencing, fencing the inner (actual) storage area is not required if the entrance(s) to such area is monitored by closed-circuit television.

g. Exterior building and door lighting shall be provided for all structures storing Category I and II items. The lighting shall be of sufficient intensity to allow detection of unauthorized activity. Switches for exterior lights shall be installed in such a manner that they are accessible only to authorized individuals.

h. Storage areas shall have a primary and backup means of communications that permit notification of emergency conditions. The backup system shall be a different mode than the primary. Radio may be one of the modes of communication. The communication system shall be tested daily.

CHAPTER 13: MAIL ROOMS

A. Physical Security Standards.

1. Central mail rooms will be designated and posted as Controlled Areas.

2. All other subordinate mail handling activities will establish entry control procedures and comply with the administrative procedures outlined in applicable DoD and DLA mail handling directives.

B. Procedures.

1. Mail operations and security procedures will be conducted in accordance with reference DoDI 4525.08, *DoD Official Mail Management*, DoD 4525.08M, *DoD Official Mail Manual*, and DLA Instruction 4212, *Official Mail* (http://www.acq.osd.mil/log/tp/452508p_1.pdf / http://www.dtic.mil/whs/directives/corres/pdf/452508p.pdf / https://headquarters.dla.mil/DES/policy/i4212.htm).

2. Central mail rooms that store registered or certified official mail overnight will be equipped with a security container that meets the requirements of DoD 5200.1-R, *Information Security Program*.

3. Automated, unmanned, self-propelled delivery systems will not be used for delivery of accounted mail, i.e., registered, certified, insured, special delivery, etc. Further, the automated system will not be used for delivery of items marked POSTMASTER: DO NOT FORWARD: RETURN TO SENDER.

4. While being transported by DLA personnel, mail will be attended at all times and will be transported in a closed-body vehicle.

5. For additional information on mail rooms, refer to your installation/facility AT Plan and Appendix D, Mail Handling and Suspicious Packages.

CHAPTER 14: THREAT ASSESSMENT / RISK MANAGEMENT

General.

1. It is incumbent on Chiefs, Security and Emergency Services/Chiefs, Security Services to adapt the standards, methods, and minimum requirements prescribed in this manual to the particular site or situation at hand, as required by local conditions. Threat may necessitate employing physical security measures beyond the scope of this manual; however, the minimum requirements outlined in this manual must be adhered to regardless of the threat.

a. Threat situations including bomb threats, hostage situations, and terrorist actions threaten the safety of DLA personnel and interrupt essential DLA operations. Therefore, positive action must be initiated to protect resources and minimize disruption of normal operations. These types of situations can be minimized by tightening security measures, restricting access to critical areas by unauthorized personnel, developing appropriate plans, and training personnel to cope with emergencies.

b. Each DLA PLFA and Installation will develop procedures for special threat situations to include reporting instructions. These procedures will be included in the activity's Physical Security Plan and all activity employees will be familiarized with the necessary actions to take in each situation.

c. DoDO Handbook 2000.12-H, *DoD Antiterrorism Handbook*, contains guidance for responses to force protection conditions and protection of DoD and DLA personnel.

d. For additional information on threat assessments, refer to your installation/facility Antiterrorism Plan.

2. It is imperative that the Chiefs, Security and Emergency Services/Chiefs, Security Services use the Risk Management Process in order to provide the PLFA Commander/Director the necessary information to make a decision on securing assets. For example; before installing an alarm in a particular area, other than required by directives, instructions, regulations, etc., the risk management process shall be used in order to provide the PLFA Commander/Director with the necessary information for him/her to justify or decide whether or not to add the additional alarm(s).

CHAPTER 15: PHYSICAL SECURITY SURVEYS, INSPECTIONS, AND EXERCISES

A. General.

The Physical Security Program makes use of a combined effort to evaluate activity needs and programs in support of resource protection.

1. A physical security survey (in-depth analysis) is required to determine the extent of security measures, which will be needed for protecting DLA personnel, property, and information. An inspection is a check or test against a certain set of standards or regulations to ascertain whether a security program or facility meets those standards or regulations. Both are used to evaluate the implementation of regulations, the security awareness of employees, security administration, and existing internal management controls. They should be used as tools by the Chief, Security and Emergency Services/Chief, Security Services to carry out his/her oversight responsibilities.

2. Survey Uses. Survey results are used for the following.

a. Determine whether the activity/program adequately protects assigned resources from criminal and terrorist acts.

b. Recommend program improvements.

c. Provide feedback for command action.

B. Types of Surveys.

1. Initial (Baseline) Survey (Security Engineering). The installation/facility physical security specialist and facility engineer personnel conduct detailed initial surveys of installation and activity facilities to assess physical security/force protection/antiterrorism requirements and capabilities.

a. The initial physical security survey is conducted prior to constructing, leasing, acquiring, modifying, or occupying a facility or area. It describes any modification required to raise the level of security commensurate with the levels of criticality and vulnerability. At a minimum, the initial survey must address the minimum-security requirements.

b. All new or remodeled facilities covered under this instruction are required to have initial surveys conducted prior to storage of resources. Facilities not meeting minimum requirements will be brought up to standards before storage of resources. The Chief, Security and Emergency Services/Chief, Security Services and the owning activity must keep the survey report for the life of the facility. ***NOTE: If an initial survey is lost, the installation/facility physical security specialist and facility engineers must conduct another survey and place it on file.***

2. Triennial Survey. The installation/facility physical security specialist conducts triennial physical security surveys for all Restricted and Controlled Areas. (These areas are self-inspected annually by Restricted/Controlled Area monitors)

3. Follow-up Survey:

a. When recommendations are made in the initial physical security survey, a follow-up survey is conducted to ensure the completion of modifications. This survey should be conducted before acceptance of the property or occupancy.

b. At the discretion of the Chief, Security and Emergency Services/Chief, Security Services, a follow-up survey may be conducted on facilities/areas where significant discrepancies were observed during the initial or periodic survey and corrective actions must be monitored.

4. Supplemental Survey. The supplemental survey is conducted when changes in the organization, mission, facility, or the threat level of the facility alter or affect the security posture of the facility or area. The Chief, Security and Emergency Services/Chief, Security Services may require that facilities undergo a supplemental survey when there is a change of the overall threat level to all survey facilities, such as the terrorist acts of September 11, 2001.

5. Special Survey. The special survey is conducted to examine or resolve a specific issue, such as when there is a request for a Sensitive Compartmented Information (SCI) accredited facility or there is a need to investigate or assess damage resulting from an incident.

C. Inspection.

Inspections, which may be announced or unannounced, are usually conducted to determine the extent of compliance with security regulations or procedures, including those recommended during surveys. The physical security specialist shall inspect facilities and programs under the security offices' cognizance as often as necessary to ensure compliance with the provisions of the applicable directives. The inspections should result in written inspection reports.

D. Survey and Inspection Reports.

1. Survey and inspection reports may be completed on a single building, facility, room, site, or an entire installation. As a minimum, reports must include the following.

a. A complete description of the facility being surveyed.

b. Compliance with physical security standard.

c. Evaluation of methods for documenting training for assigned personnel.

d. Compliance with administrative security requirements such as possession of local plans, instructions, handbooks, required letters, etc.

e. Assessment of non-duty hour and/or nighttime security standards.

f. Circulation control assessment.

g. Recommended corrective actions.

2. Reports should be produced within 90 working days of completion of the survey or inspection. The report should be distributed to the office, facility, or manager in a timely manner and require a response to any recommendations. Copies of final inspection reports shall be maintained by the

installation office of Security and Emergency Services. Reports of surveys and inspections of Government-owned facilities conducted to ensure adequacy of protective and preventive measures taken against hazards of fire, explosion, and accidents, and to safeguard information and facilities against sabotage and unauthorized entry. Destroy when 3 years old or upon discontinuance of facility, whichever is sooner.

E. Robbery and Penetration Exercises.

1. Funds facilities storing over $25,000 must be exercised annually. Facilities storing less than $25,000 are exempt from exercises; however, fund facility custodians may request exercises through the local security forces if they so desire.

2. As determined locally, penetration exercises shall be conducted on Restricted and Controlled Areas. These exercises shall test the response of owner/user personnel and security forces.

F. COMSEC and SIPRNET.

Contact your local J6 Information Operations, COMSEC manager and Information Security Office for guidance on securing and managing COMSEC equipment at your area.

CHAPTER 16: WAIVERS, VARIANCES, AND EXCEPTIONS

A. General.

The DLA Physical Security Waiver Program is designed to assist activities in effectively accomplishing their mission while providing a method of accountability throughout DLA. It supports DLA activity alternate physical security measures employed to provide a degree of security equivalent to that prescribed. Deterrence is achieved by implementing and practicing security programs/procedures that present hostile persons or groups with unacceptable risks and penalties if they attempt to breach the security system. DLA operational requirements and the need to moderate manpower and material costs dictate prudence in achieving a balance between security and acceptable degrees of risk.

B. Types of Deviation.

1. The security deviation program formalizes security program risk acceptance. The inability to meet minimum DoD and DLA security requirements results in a higher security risk. Activities must implement the security deviation program where resources are not protected at the required protection level.

2. Security deviation provides a management tool for DLA Activities to review, monitor, plan, and program for corrections to deviations from requirements. The ultimate goal of the program is to ensure the correction of all correctable deviations as quickly as possible.

3. Security deviation categories.

a. *Exception.* A permanent deviation that is requested when a security-threatening condition is not correctable or when the office requesting the deviation states that correcting a problem would result in unacceptable cost. Exceptions are permanent but will be reviewed by DLA Installation Support, Security and Emergency Services every 3 years to ensure that the deficient conditions still exist and that compensatory measures are still adequate. Conditions approved as exceptions require compensatory measures.

b. Waiver. A temporary deviation that is requested when a correctable, security threatening condition exists. Conditions approved as waivers require compensatory measures. Waivers are valid for no more than 1 year.

c. Variance. A technical deviation that is requested when a condition exists without threatening security but technically differs from established requirements. Conditions approved as variances do not require compensatory measures or corrective actions. Variances are approved for an indefinite time period.

C. Procedures.

1. DLA Installation Support, Security and Emergency Services ensures that security policies and standards meet national security objectives, and that security products and services provided satisfy customer needs and expectations.

2. DLA Installation Support, Security and Emergency Services will continue to conduct Security Program Reviews (SPRs) in accordance with DLAI 4301. Results of these reviews will be provided to

the DLA Installation Support Site Directors and activity Chief, Security and Emergency Services/Chief, Security Services.

3. The Chief, Security and Emergency Services/Chief, Security Services will act as the primary advisor for security issues to the DLA Installation Support Site Directors, as well as all DLA Activity heads at the supported location(s). He/she will oversee implementation of the DLA Security Waiver Program at the supported activity.

4. The Chief, Security and Emergency Services/Chief, Security Services and security personnel may be issued identification credentials in accordance with DLA Instruction 4313, *Issuance of Credentials to DLA Security Personnel*. The Chief, Security & Emergency Services/Chief, Security Services will review and address specific needs and possible waiver issues with DLA HQ.

5. DLA Installation Support, Security and Emergency Services is the office of primary responsibility for approving or disapproving security deviation requests.

6. Requests for security deviations will be reviewed and signed by the Head of the DLA activity, Site Director, or their appointed Deputy using DLA Form 1885, Requests for Deviation from Security Criteria. It will then be forwarded to DLA Installation Support, Security and Emergency Services for further processing. The request will include:

a. A statement of the problem or deficiency that constitutes standards below those cited applicable directives or instructions and identification of the reference from which temporary relief is requested.

b. A description of measures in effect that compensate/mitigate for noncompliance with required standards of protection.

c. Reasons why the activity cannot comply with the requirements of this manual. An explanation of the plan or program that will fulfill the prescribed security requirement will be included in the request for waiver.

d. Estimated date the deficient conditions will be corrected.

e. If the vulnerability is classified, DLA Form 1885 shall be marked and classified appropriately (For Official Use Only, Secret, etc). Guidelines for classifying vulnerabilities can be found in the Defense Threat Reduction Agency Security Classification Guide for Vulnerability Assessments.

f. Deviations are not required for deficiencies that can be corrected within 90 days of discovery.

g. Security Deviation Renewals and Expirations. Request for deviation renewals or extensions will be submitted to DLA Installation Support, Security and Emergency Services no later than 60 days prior to the expiration date.

h. DLA Installation Support, Security and Emergency Services will be notified within five days, in writing, whenever a deficiency for which a deviation has been granted, is corrected.

D. Compensating for Security Deviations.

Compensatory measures, by definition, are different than security measures normally in-place. Although different, they must provide a comparable level of security. Security forces, facilities, equipment, and procedures that are already required are not normally adequate as compensatory measures. Additionally, instructions consisting mainly of orders to "increase vigilance" are inadequate. Additional forces, equipment, procedures, etc., are usually necessary to ensure comparable security. However, there are some instances when existing forces may be used to compensate temporarily for deviations. For example, if the IDS for a sector fails and the existing alarm monitor can continuously provide surveillance to the failed sector either by line of sight or camera, that alarm monitor may be used to compensate for the deviation until more permanent actions can be taken.

E. AA&E Waiver Process.

DLA components may deviate from the construction standards of this Manual for new and existing facilities if they specify equivalent levels of protection. However, deviations from the non-construction requirements prescribed herein must be requested in writing from activities storing in accordance with AA&E procedures under the following provisions:

1. Blanket waivers and exceptions shall not be authorized. Waivers shall be granted for a 12 month period and shall specify the approval rationale as well as the equivalent compensatory measures that will substitute for the waived requirement(s).

2. Exceptions shall be granted only when compliance with a requirement from this manual would unduly impede mission performance as described and documented in the exception request. As with waivers, approved exceptions shall specify the rationale for granting the exception as well as the alternative or compensatory security measure(s) that will substitute for the excepted security requirement(s). Exceptions shall be reviewed every three years by DLA Installation Support, Security and Emergency Services.

3. Waivers and exceptions requests involving commercial transportation of AA&E shall be coordinated in advance with the Military Traffic Management Command. Copies of such approved waivers and exceptions shall be forwarded to the Commander, Military Traffic Management Command, ATTN: MTIN, 5611 Columbia Pike, Falls Church, VA 22041-5050.

4. Deficiencies (noncompliance with the requirements of this manual) that will be corrected within 90 days shall not require a waiver; however, compensatory measures shall be taken during the 90 day interval.

CHAPTER 17: WORKING GROUPS

A. General.

1. The changing methods of attack used by our adversaries require us to consider the nontraditional ways in which we may be attacked and how to counter these elusive threats. Evolving methods of attack vary from standoff to suicide, single to simultaneous, automobiles to boats to airplanes—all designed to catch victims off guard. Because of ever-changing tactics, we must be increasingly vigilant and corroborate, using all the various expertise available to out-think our enemies and negate their intentions.

2. DLA Installation Support, Security and Emergency Services at all levels must aggressively and effectively execute their force protection responsibilities and programs. Installation Commanders/Directors are responsible for protecting their people and the resources used to perform day-to-day operations. Force Protection and a secure environment is accomplished through planned and integrated application of intelligence, counterintelligence, risk management, combating terrorism, force health protection, integrated base defense, information security, operations security, law enforcement liaison and the integration of installation working groups. All Physical Security specialists at DLA locations are encouraged to attend working groups in their area, should time and funding permit. We are obligated by our past, present, and future to ensure force protection is a part of DLA's culture.

B. HQ DLA Physical Security Working Groups.

1. DLA Access Control Working Group (ACWG): The ACWG is established under the auspices of the Director, DLA Installation Support, to provide a mechanism to ensure consistency in the implantation of DLA's Installation Access Control Program. The group encourages the use of commercial off-the-shelf (COTS) technology solutions and equipment to implement a standardized PACS across the Agency. The group consists of members from DLA Installation Support, Security and Emergency Services (HQ and Field), General Counsel, Information Operations, and Financial Operations.

2. DLA Physical Security/Antiterrorism Working Group (PSATWG): A forum of DLA Installation Support, Security and Emergency Services Physical Security Specialist to ensure information sharing and open communication between DLA HQ and Field Activities. The PSWG will meet on a bi-monthly basis and will provide personnel an opportunity to raise physical security concerns and issues and solve problems within an enterprise framework.

C. Installation/Facility Working Groups.

Force Protection Working Group (FPWG): A cross-functional working group whose purpose is to conduct risk assessment and risk management. In addition, recommend mitigating measures to the Commander/Director of DLA Installations/Facilities. The FPWG also plays a major role in contingency planning, analyzes threats, assists in developing force protection actions and civil defense measures, and recommends Force Protection Condition (FPCON) security measures.

1. Each FPWG should have a sub-working group to handle ESS. Topics discussed should include IDS, CCTV, connectivity, alarm priority, etc. All owner/users of alarmed areas should attend these meetings.

2. Disposition of Working Group files/records. Working Group program files/records shall be destroyed 2 years after termination of the program effort in accordance with DLA Records Schedule 150.01.

CHAPTER 18: PHYSICAL SECURITY EDUCATION AND TRAINING PROGRAM

A. General.

Commanders, Directors, and supervisors at all levels must ensure security training is provided. Chiefs, Security and Emergency Services/Chiefs, Security Services for all DLA Activities will implement a Security Education and Training Program. The purpose of the program is to educate activity employees on security policies and procedures, increase their awareness of security concerns, and enlist their assistance in the protection of DLA resources.

B. Objective.

The objective of the security education and training program is to instill in every employee a sense of responsibility for the security of resources and to provide training enabling them to react quickly and correctly to threats directed at those resources. Protection of government property is the responsibility of all employees. All employees must shoulder their share of security responsibility. It is incumbent upon all supervisors to give security awareness the full measure of consideration it deserves and to emphasize its importance to subordinates.

C. Elements.

The DLA Physical Security Awareness Training Program will include at a minimum, the following elements:

1. Regular briefings to activity employees on security procedures and current security concerns.

2. Posting of procedures and policies near employee workstations.

3. Use of posters, videos, and other media to increase awareness and interest in the security of the activity.

4. Personal attention to employee's concerns and development of personal contacts.

5. Regular reports on scheduled security improvements and enhancements to enlist the support of activity employees and limit resistance to such projects.

6. Crime Prevention

7. Reporting suspicious activity

D. Implementing the Program.

Design the program so unit personnel attain the skills they need to apply security techniques pertaining to their particular job or assignment. For example, an administrative specialist who does not work in a Controlled Area will not need the same depth of understanding as a worker whose place of duty is within a Controlled Area. The program consists of Phase I, Orientation Training, and Phase II, Continuation Training. Programs should follow the guidance outlined in the paragraphs below.

1. **Phase I, Orientation Training.** This phase is directed toward security procedures and requirements peculiar to the field activity of assignment (the installation, depot, GSA facility, etc), and the job of each individual. All employees will receive an initial security indoctrination briefing during their first month of employment. Everyone should have a general knowledge of the following.

a. The threat and how it applies to their area of responsibility.

b. Contents of the security plan and how it applies to their area of responsibility.

c. The security reporting and alerting system, to include methods of notifying the security operations center during emergency situations.

d. Crime prevention awareness and the reporting of suspicious activity.

e. Common security hazards

f. Installation/Facility site-specific access controls, vehicle control, and property accountability or package inspection programs.

g. Additionally, persons granted unescorted entry to a Restricted or Controlled Area receive orientation on the following:

(1) Entry control procedures, including verification of the right and need to be in the area

(2) Responsibilities and duties of an escort official

(3) Methods used to gain authorized entry to the area.

2. **Phase II, Continuation Training.** All employees will receive continuation security training at least once per year. This phase is ongoing and tailored to the individual job. Phase II is designed to keep everyone apprised of threats, security procedures and responsibilities, and mission changes affecting them.

E. PLFA Commander/Director Responsibilities.

1. Develop and implement programs at the field activity level. The program must lend itself to supplementation by Staff Directors and Division Chiefs.

2. Develop tailored programs to meet the needs of employees and evaluate security awareness of installation personnel.

3. Directors and Division Chiefs implement the program by administering Phase I and II training. Use training materials applicable command-wide to present initial and recurring training to their personnel.

F. Records.

1. Records of security education and training sessions will be recorded in the DLA Learning Management System (LMS). These records will be reviewed by DLA Installation Support, Office of

Security and Emergency Services during physical security surveys and staff assistance visits to determine the effectiveness of the program and compliance with this manual.

2. Disposition of files/records. Files/records relating to the preparation, conduct and follow-up analysis of formal and informal training awareness instruction designed to acquaint individuals with the objectives, principles and methods of OPSEC programs and to maintain a sense of OPSEC awareness among military and civilian personnel assigned to DLA and PLFAs. (Destroy after 5 years or upon obsolescence or supersession per N1-361-91-007.)

APPENDIX A: GLOSSARY OF REFERENCES AND SUPPORTING PUBLICATIONS

References*:*

Internal Security Act of 1950 (50 U.S.C. 797)

DoDI 5200.08, *Security of DoD Installations and Resources and the DoD Physical Security Review Board (PSRB);* May 19, 2010. http://www.dtic.mil/whs/directives/corres/pdf/520008p.pdf

DoD 5200.08-R, *Physical Security Program;* May 27, 2009.
http://www.dtic.mil/whs/directives/corres/pdf/520008r.pdf

DoDD 2000.12, *DoD Antiterrorism Program;* August 18, 2003.
http://www.dtic.mil/whs/directives/corres/pdf/200012p.pdf

DoDD 3020.40, *DoD Policies and Responsibilities for Critical Infrastructure;* July 1, 2010.
http://www.dtic.mil/whs/directives/corres/pdf/302040p.pdf

DoDD 5105.22, *Defense Logistics Agency;* May 17, 2006.
http://www.dtic.mil/whs/directives/corres/pdf/510522p.pdf

DoDD 5205.02, *DoD Operations Security (OPSEC) Program;* March 6, 2006.
http://www.dtic.mil/whs/directives/corres/pdf/520502p.pdf

DoDI 2000.16, *DoD Antiterrorism (AT) Standards;* December 8, 2006.
http://www.dtic.mil/whs/directives/corres/pdf/200016p.pdf

DoDI 2000.18, *DoD Installation CBRNE Guidelines;* December 4, 2002.
http://www.dtic.mil/whs/directives/corres/pdf/200018p.pdf

DoDI 4525.08, *DoD Official Mail Management*; August 11, 2006.
http://www.dtic.mil/whs/directives/corres/pdf/452508p.pdf

DoDI 5210.65, *Minimum Security Standards for Safeguarding Chemical Agents;* March 12, 2007.
http://www.dtic.mil/whs/directives/corres/pdf/521065p.pdf

DoD 4140.1-R, Supply Chain Material Management Regulation, May 23, 2003
http://www.acq.osd.mil/log/sci/exec_info/drid/p41401r.pdf

DoD 4160.21-M, Defense Material Disposition Manual; August 18, 1997.
http://www.dtic.mil/whs/directives/corres/pdf/416021m.pdf

DoD 4525.08-M, DoD Official Mail Manual; December 26, 2001.
http://www.dtic.mil/whs/directives/corres/pdf/452508m.pdf

DoD 5220.22-M, National Industrial Security Program Operating Manual (NISPOM); February 28, 2006.
http://www.dtic.mil/whs/directives/corres/pdf/522022m.pdf

DoD 5100.76-M, *Physical Security of Sensitive Conventional Arms, Ammunition, and Explosives (AA&E);* August 2000. http://www.dtic.mil/whs/directives/corres/pdf/510076m.pdf

DoD 4500.9-R, *Defense Transportation Regulation*

DoD 5200.1-R, *Information Security Program;* January 14, 1997.
http://www.dtic.mil/whs/directives/corres/pdf/520001r.pdf

DoD 5200.2-R, *Personnel Security Program*; February 23, 1996.
http://www.dtic.mil/whs/directives/corres/pdf/520002r.pdf

DoD 6055.9-STD, *DoD Ammunition And Explosives Safety Standards,* July 1999
http://www.ddesb.pentagon.mil/60559s99.pdf

DoD 7000.14-R, *DoD Financial Management Regulation;* Date varies by volume.
http://www.dtic.mil/whs/directives/corres/html/700014r.htm

DoDD 5015.02, *DoD Records Management Program;* March 6, 2000.
http://www.dtic.mil/whs/directives/corres/pdf/501502p.pdf

DoDO Handbook 2000.12-H, *DoD Antiterrorism Handbook;* February 2004.
http://www.dtic.mil/whs/directives/corres/pdf/200012h.pdf

Unified Facilities Criteria (UFC) 4-010-01, *DoD Minimum Antiterrorism Standards For Buildings.*
http://www.wbdg.org/ccb/DOD/UFC/ufc_4_010_01.pdf .

Unified Facilities Criteria (UFC) 4-010-02, *DoD Minimum Antiterrorism Standoff Distances For Buildings.* http://www.wbdg.org/ccb/DOD/UFC/ufc_4_010_02.pdf.

MIL Handbook 1013/1A, *Design Guidelines for Physical Security of Fixed Land-Based Facilities.*
http://www.wbdg.org/ccb/NAVFAC/DMMHNAV/1013_1a.pdf.

ICD 705, *Sensitive Compartmented Information Facilities,* May 26, 2010.
http://www.fas.org/irp/dni/icd/icd-705.pdf

ICS 705-1, *Physical and Technical Security Standards for Sensitive Compartmented Information Facilities*, September 17, 2010
http://www.fas.org/irp/dni/icd/ics-705-1.pdf

ICS 705-2, *Standards for the Accreditation and Reciprocal Use of Sensitive Compartmented Information*, September 17, 2010
http://www.fas.org/irp/dni/icd/ics-705-2.pdf

MCR 55-18, Operational Procedures for Aircraft Carrying Hazardous Materials

MIL STD 21313G, Pad Lock Sets - Individually Keyed and Keyed Alike

MIL STD 35647E, Pad Lock, Key Operated

Federal Property Management Regulations (FPMR), *Title 41 Code of Federal Regulations (C.F.R.), Subpart 101-20.1*

DLA Directive (DLAD) 5025.30, DLA Instructions: *Physical Security Program* (4306)*; Security and Emergency Services* (4301)*; Information Security Program* (6304)*; Force Protection and Security Operations* (4302)*; Carrying of Firearms and Use of Force* (4310)*; Issuance of Credentials to DLA Security Personnel (4313); Operations Security* (6305)*; Personnel Security Program* (4314)*; Vehicle Registration* (4309)*; Official Mail* (4212).

DLAR 4145.11, *Safeguarding of DLA Sensitive Inventory Items, Controlled Substances, and Pilferable Items of Supply* (Joint Regulation). http://www.dla.mil/dlaps/dlar/r4145.11.pdf

DLA Security Forces Policies and Procedures Manual

Washington Headquarters Service (WHS) Administrative Instruction 15, Volume 1, Office of Secretary of Defense (OSD) Records Management Program

Forms Referenced or Prescribed:

DD Form 200, Financial Liability Investigation of Property Lost

DD Form 577, Signature Card

DD Form 2220, DoD Registered Vehicle Decal

Standard Form 700, Security Container Information

Standard Form 702, Security Container Check Sheet

Optional Form 7, Property Pass

DLA Form 584, Visitor Register

DLA Form 1610, Key Repository Index

DLA Form 1610a, Key Repository Accountability Record

DLA Form 1610b, Delegation of Authority-Key Control

DLA Form 1610c, Key Control Register

DLA Form 1617, Cargo Movement and Seal Record

DLA Form 1749, Vehicle Registration Log

DLA Form 1813, Request and Approval For Off-Site Processing

DLA Form 1885, Request For Deviation From Security Criteria

DLA Form 1886, Robbery Checklist

DLA Form 1922, Request for Open Storage Approval

APPENDIX B: DEFINITIONS

Activity (ies). 1. A unit, organization, or installation performing a function or mission, 2. A function, mission, action, or collection of actions.

Ammunition. A device charged with explosives, propellants, pyrotechnics, initiating composition, riot control agents, chemical herbicides, smoke and flame, for use in connection with defense or offense, including demolition. Excluded from this definition are devices charged with chemical agents defined in JCS Pub. 1 and nuclear or biological material. Ammunition includes cartridges, projectiles, including missile rounds, grenades, mines, and pyrotechnics together with bullets, shot and their necessary primers, propellants, fuses, and detonators individually or having a unit of issue, container, or package weight of 100 pounds or less. Blank, inert training ammunition and caliber .22 ammunition are excluded.

Antiterrorism. Defensive measure used to reduce the vulnerability of individuals and property to terrorist acts, to include limited response and containment by military forces.

Approving Authority. Official designated by the Head of the DLA PLFA or the DLA Installation Commander to approve issuance of the DLA Identification Card.

Arms. A weapon that will or is designated to expel a projectile or flame by the action of the explosive, and the frame or receiver of any such weapon.

Badge. A security credential that is worn on the possessor's outer garment and validates (his or her) authority for access to a secure area.

Bulk Storage. Storage in a facility above the using or dispensing level specifically applicable to logistics warehouse and depot stocks. This applies to activities using controlled medical substances and items (such as pharmacies, wards, or clinics) only when a separate facility (building or room) is used to store quantities that exceed normal operating stocks.

Cable Seal Lock. A seal in which the cable is passed through the locking hardware of a truck trailer or railcar door and the bullet nose is inserted into the barrel and the end of the cable until securely anchored. Once locked, any force exerted to separate the lockpoint from the lockbody will strengthen its connection. (DOD 5100.76–M)

Chemical, Biological, Radiological, Nuclear, and High-Yield Explosive (CBRNE) Incident. The deliberate or inadvertent release of chemical, biological, radiological, nuclear or high-yield explosive devices with potential to cause significant numbers of casualties and high levels of destruction.

Clear Zone. An area on both sides of a perimeter barrier that provides an unobstructed view of the barrier and the ground adjacent to it.

Closed Circuit Television. Television that serves a number of different functions, one of which is physical security. As it pertains to the field of physical security, CCTV is used to augment, not replace, existing intrusion detection systems (IDS) or security patrols. It is not used as a primary sensor, but rather as a means of assessing alarms. CCTV also may be used as a surveillance means, but if used in this way, it will augment, not replace, existing IDS.

Closed Installation. A DLA-operated installation or activity to which access is controlled at all times by perimeter barriers with limited, manned entry control points.

Combating Terrorism. Actions, including AT and CT, taken to oppose terrorism throughout the entire threat spectrum.

Compensatory Measure. An alternate physical security measure employed to provide a degree of security equivalent to that provided by a required physical security measure.

Controlled Area. This area is designated by a Commander or Director, wherein sensitive resources, information or operations occur and requires limited and controlled access.

Controlled Medical Substance. A drug or other substance, or its immediate precursor, listed in current schedules of 21 USC 812 in medical facilities for the purpose of military treatment, therapy, or research. Categories listed in this section are narcotics, amphetamines, barbiturates, and hallucinogens.

Counterterrorism. Offensive measures taken to prevent, deter, and respond to terrorism.

DLA Installation. Any real DoD property under the operational control of DLA. This includes supply centers, depots, arsenals, plants (both contractor and Government operated), and other special mission facilities, as well as those used primarily for military purposes.

Electronic Security Systems (ESS). That part of physical security concerned with the safeguarding of personnel and property by use of electronic systems. These systems include, but are not limited to, intrusion detection systems (IDS), automated entry control systems (AECS), and video assessment systems.

Emergency Responders. Firefighters, law enforcement/security personnel, and emergency medical technicians, emergency management and operations personnel, Explosive Ordnance Disposal (EOD) personnel, physicians, nurses, medical treatment providers at medical treatment facilities, disaster preparedness officers, public health officers, bio-environmental engineers, and mortuary affairs personnel.

Entry Control. Security actions, procedures, equipment, and techniques, employed within secure areas to ensure that persons who are present in the areas at any time have authority and official reason for being there.

Escorted Personnel. Those individuals allowed access to a secure area who are escorted at all times by a designated person.

Exception. A permanent deviation that is requested when a security-threatening condition can't be corrected or when correcting a problem would result in exorbitant cost. Exceptions are granted for no more than 3 years. Conditions approved as exceptions require compensatory measures.

Explosives. Any chemical compound, mixture or device, the primary or common purpose of which is to function by explosion. The term includes, but is not limited to, individual land mines, demolition charges, blocks of explosives (dynamite, trinitrotoluene (TNT), C–4, and other high explosives), and other explosives consisting of 10 pounds or more; for example, gunpowder or nitro guanidine.

Facility(ies). A real property entity consisting of one or more of the following: a building, a structure, a utility system, pavement, and underlying land.

First Responders. Firefighters, law enforcement and/or security personnel, emergency medical technicians, and EOD personnel (for suspected explosive CBRNE events) that provide the initial, immediate response to a major incident (such as CBRNE).

Force Protection. Security program developed to protect military and civilian employees, family members, facilities, and equipment, in all locations and situations. This is accomplished through the planned integration of combating terrorism, physical security, operations security, protective services and security force operations, all supported by foreign intelligence, counterintelligence and other security programs.

Government Funds. Funds controlled by DLA personnel that include, without being limited to, revenues and funds of the United States or any of its officers, agents or employees. All appropriated, nonappropriated and other Government funds or negotiable instruments, except checks marked payable to the United States Treasury or stamped "For Deposit Only."

High Risk Personnel. Personnel who, by their grade, assignment, value, location, or specific threat, are more likely to be attractive or accessible terrorist targets.

Installation. A grouping of facilities, located in the same vicinity, which support particular functions. Installations may be elements of a base.

Intrusion Detection System (IDS). The combination of electronic components, including sensors, control units, transmission lines, and monitoring units integrated to be capable of detecting one or more types of intrusion into the area protected by the system and reporting directly to an alarm monitoring station.

Issuing Authority. Official designated by the DLA PLFA Commander/Site Director to issue the DLA Identification Card.

Key and Lock Control System. A system of identifying both locks and their locations and personnel in possession of keys and/or combinations.

Key Card. A card used with an automated access control system to control access into specific areas of DLA Activities. The card will normally contain embedded information in the form of a magnetic strip, bar code, or proximity chip that when read by the card reader allows or denies entry/exit to the card holder.

Key Control Officer. The person (normally in the Command Support Office or Directorate of Installation Services) designated in writing by the Head of the DLA Activity to manage and direct the Key and Lock Control Program.

Key Custodian. The person designated to manage a key repository within the Key and Lock Control Program.

Open Installation. Installations or activities that do not qualify as closed or limited access posts. Access to the installation or activity is not controlled during or after normal duty hours.

Owner-User. The organization/individual responsible for an assigned resource.

Physical Security. That portion of security concerned with procedures and physical measures designed to safeguard personnel, property, and operations; to prevent unauthorized access to equipment, facilities,

material, and information; and to protect against espionage, terrorism, sabotage, damage, misuse, and theft.

Physical Security Plan. A comprehensive written plan providing proper and economical use of personnel, land, and equipment to prevent or minimize loss or damage from theft, misuse, espionage, sabotage, and other criminal or disruptive activities.

Primary level field activity:
Protection In Depth. A system providing several supplementary security barriers. For example, a perimeter fence, a secure building, a vault, and a locked container provide four layers of protection.

"Q" Controlled Medical Items. All standard drug items identified as Note Q in the Federal Supply Catalog, Nonstandard Drug Enforcement Administration (DEA) Schedule III, IV, V Controlled Substances.

"R" Controlled Medical Items. All items identified as Note R in the Federal Supply V Catalog Nonstandard DEA Schedule II Controlled Substances.

Restricted Area. An area in which there are special restrictive measures employed to prevent or minimize incursions and/or interference, where special security measures are employed to prevent unauthorized entry.

Risk. A measure of consequences of peril, hazard or loss, which is incurred from a capable aggressor or the environment (the presence of a threat and unmitigated vulnerability).

Risk Assessment. A defined process used to fuse the procedures of analyzing threat, risks, and vulnerabilities, into a cohesive, actionable product.

Risk Factors. Elements that make up the total degree of resource loss liability. Factors to be considered in a risk assessment include the importance of the resource to mission accomplishment; the cost, volume, criticality and vulnerabilities of the resources; and the severity of threats to the resources.

Risk Management. Process and resultant risk of systematically identifying, assessing and controlling risks. PLFA Commanders/Directors are required to identify critical assets and their subsequent protection requirements, including future expenditures required for the protection requirements.

Seal. A device to show whether the integrity of a shipment has been compromised. Seals are numbered serially, are tamperproof, and shall be safeguarded while in storage. The serial number of a seal shall be shown on Government Bills of Lading (GBL). A cable seal lock provides both a seal and locking device.

Sealed Containers. Wooden boxes, crates, metal containers, and fiber containers sealed in a way to show when the containers are tampered with after sealing. The method of sealing depends of the type of construction of the containers. Sealing may be by metal banding, nailing, airtight sealing, or wax dripping (for fiber containers). In key control, a sealed container is also a locked key container or a sealed envelope containing the key or combination to the key container.

Secure Area. An area, building, structure, or room under DoD control that requires special security measures to protect U.S. Government resources contained therein.

Security Badge. A locally-developed, unique badge used to control access into, and facilitate personnel identification within, specific areas of DLA Activities.

Security Deviation. A management tool for DLA Activities to review, monitor, plan, and program for corrections to deviations from security requirements. The ultimate goal of the program is to ensure the correction of all correctable deviations as quickly as possible.

Security Engineering. The application of engineering principles to the protection of assets against various threats through the application of construction and equipment application.

Security Executive Committee. The single governing body responsible to the PLFA Commander/ Director for installation/activity security.

Security-in-Depth. A determination by the senior activity official that an activity's security program consists of layered and complimentary security controls sufficient to deter, detect, and document unauthorized entry and movement within the activity. Examples include the use of perimeter fences, employee and visitor access controls, use of an intrusion detection system, random guard patrols, and closed circuit video monitoring or other safeguards that mitigate a vulnerability.

Security Program Review. A formal, recorded assessment by higher headquarters of the installation's overall security program.

Security Working Group. Groups established to identify mission-essential resources or test program effectiveness and work under the direction and authority of the Security Executive Committee.

Site: Location of a DLA entity

Survey. A formal, recorded assessment (by means of on-site inspection) conducted locally by the security staff of physical procedures and measures implemented by a facility, unit, directorate, installation or activity to protect its assets.

Temporary Secure Area. An area, building, structure, or room, which for unscheduled or intermittent periods, is used as a secure area.

Terrorism. The calculated use of violence or the threat of violence to inculcate fear; intended to coerce or to intimidate governments or societies in the pursuit of goals, that are generally political, religious, or ideological.

Threat. The perceived imminence of intended aggression by a capable entity to harm a nation, a government or its instrumentalities, such as intelligence, programs, operations, people, installations, or facilities.

Threat Analysis. The continual process of compiling and examining all available information concerning the capability, activity, and intention of potential aggressors, which supports the deployment and degree of countermeasure requirements to address the perceived threat.

Threat Assessment. A resultant product of the defined process used to conduct a threat analysis and develop an evaluation of a potential threat. Also, it is the product of a threat analysis for a particular unit, installation, or activity.

Utility Area. An area containing equipment that provides an essential service, such as heat, water, or power, and that requires security measures to protect the equipment from destruction or damage.

Variance. A technical deviation that is requested when a condition exists that doesn't threaten security but technically differs from established requirements. Conditions approved as variances don't require compensatory measures or corrective actions. Variances are approved for an indefinite time period.

Visitor. Any individual, military or civilian, not assigned to or employed within an installation, activity, or area to which access is requested.

Vulnerability. A situation or circumstance, which left unchanged, may result in the degradation, loss of life, or damage to mission-essential resources.

Vulnerability Assessment. The comprehensive evaluation of an installation, facility, or activity to determine preparedness to deter, withstand, and /or recover from the full range of adversarial capabilities based on the threat assessment, compliance with protection standards, and risk management.

Waiver. A temporary deviation that is requested when a correctable, security-threatening condition exists. Conditions approved as waivers require compensatory measures. Waivers are granted for no more than 1 year.

APPENDIX C: SAMPLE PHYSICAL SECURITY PLAN

Note: Plan still under revision to properly align with DLA Physical Security Manual

Copy No. _____
Issuing Headquarters
Place of Issue
Date of Issue

Physical Security Plan

Part I. General.

1. Purpose. State the plan's purpose.

2. Area Security. Define the areas, buildings, and other structures considered critical and establish priorities for their protection.

3. Control Measures. Define and establish restrictions on access and movement into critical (i.e. Restricted and Controlled Areas) areas.

a. Categorize restrictions as to personnel, materials, and vehicles: (1)

(1) Personnel access:

(a) Establishment of controls pertinent to each area or structure.

- Authority/for access
- Criteria for access.
  - Unit personnel.
  - Visitors.
  - Maintenance personnel.
  - Contractor personnel.
  - National Guard.
  - Emergency response teams (police, fire, ambulance).

(b) Identification and control.

- Description of the system to be used in each area. If a badge system is used, a complete description covering all aspects should be used in disseminating requirements for ID and control of personnel conducting business on the installation.

- Application of the system:
  - Unit personnel.
  - Visitors to secure areas.
  - Visitors to administrative areas.
  - Vendors, tradesmen and so forth.
  - Contractor personnel.
  - Maintenance or support personnel.
  - Fail-safe procedures during power outages.

(2) Material control.

(a) Incoming.

- Requirements for admission of material and supplies.
- Search and inspection of material for possible sabotage hazards.
- Special controls on delivery of supplies or personal shipments in restricted areas.

(b) Outgoing.

- Documentation required.
- Controls.
- Classified shipment not involving nuclear/chemical material.

(c) Hazardous Material (HAZMAT).

- Controls on movement of HAZMAT on the installation.
- Controls on shipments or movement of training HAZMAT.
- Controls on pickup or delivery of HAZMAT outside the installation.

(3) Vehicle control.

(a) Policy on search of military and privately owned vehicles.

(b) Parking regulations.

(c) Controls for entrance into restricted and administrative areas:

Military vehicles.

POVs.

Emergency vehicles.

Vehicle registration.

b. Indicate the manner in which the following security aids will be implemented on the installation.

(1) Protective barriers:

(a) Definition.

(b) Clear zones.

- Criteria.
- Maintenance.

(c) Signs.

- Types.
- Posting.

(d) Gates.

- Hours of operation.
- Security requirements.
- Lock security.
- Barrier plan.

(2) Protective lighting system:

(a) Use and control.

(b) Inspection.

(c) Action taken in case of commercial power failure.

(d) Action taken in case of failure of alternate power source.

(3) Emergency lighting system:

(a) Stationary.

(b) Portable.

(4) IDSs:

(a) Security classification.

(b) Inspection.

(c) Use and monitoring.

(d) Action taken in case of alarm conditions.

(e) Maintenance.

(f) Alarm logs or registers.

(g) Tamper-proof provisions.

(h) Monitor-panel locations.

(5) Communications:

(a) Locations.

(b) Use.

(c) Tests.

(d) Authentication.

(6) Security Forces: General instructions that would apply to all security-force personnel (fixed and mobile). Detailed instructions such as special orders and SOP information should be attached as annexes. Security force facets include—

(a) Composition and organization.

(b) Tour of duty.

(c) Essential posts and routes.

(d) Weapons and equipment.

(e) Training.

(f) Use of MWD teams.

(g) Method of challenging.

(h) Alert forces:

- Composition.
- Mission.
- Weapons and equipment.
- Location.

(7) Contingency plans: Required actions in response to various emergency situations. Detailed plans for situations (counterterrorism, bomb threats, hostage negotiations, disaster, fire, and so forth) should be attached as annexes.

(a) Individual actions.

(b) Alert-force actions.

(c) Security-force actions.

(8) Use of air surveillance.

(9) Coordinating instructions. Matters that require coordination with other military and civil agencies such as—

(a) Adjacent installations or units.

(b) State and local agencies.

(c) Similar host-country agencies.

(d) Federal agencies.

The coordination/interaction allows for an exchange of intelligence information on security measures being used, contingency plans, and any other information to enhance local security.

On an installation, the host activity shall assume responsibility for coordinating physical-security efforts of all tenants, regardless of the components represented, as outlined in the support agreements and the host-activity security plan. Applicable provisions shall be included in, or be an appendix to, the support agreement. A formal agreement will contain definite assignment of physical-security responsibility for the terns stored. The agreement should address—

- Maximum qualities to be stored.
- Physical safeguards to be used.
- Frequency of, and responsibility for, physical inventories or reconciliations.
- Reporting of losses for investigation.
- Lock and key control.
- The unit that has overall responsibility.

Procedures for authorization and ID of individuals to receipt for and physically take custody of DLA property. The purpose of such coordination is protection in depth. Authority, jurisdiction, and responsibility must be set forth in a manner that ensures protection and a voids duplication of effort.

Part II. Annexes

Annexes to the plan should include, but are not limited to, the following.

Annex A. The installation/facility threat statement (intelligence).

Annex B. Installation access control and closure plan.

Annex C. Incident response plan.

Annex D. A bomb-threat plan. As a minimum, the bomb-threat plan should provide guidance for—

- Control of the operation.
- Evacuation.
- Search.
- Finding the bomb or suspected bomb.
- Disposal.
- Detonation and damage control.
- Control of publicity.
- After-action report.

Annex E. A disaster plan. This plan will be coordinated with disaster plans of local jurisdictions. At a minimum, the disaster plan should provide guidance for—

- Control of the operation.
- Evacuation.
- Communication.
- Control of publicity.
- After-action report.

Annex F. A civil-disturbance plan. It is the PLFA Commander's/Director's responsibility to formulate a civil-disturbance plan based on local threats. (For example, Commanders may anticipate the need to develop crowd-control procedures to handle antichemical demonstrations.)

Annex G. A resource plan to meet the minimum-essential physical-security needs for the installation or activity.

Annex H. Implementation of force protection condition measures.

Annex I. A communication plan. This plan is required to establish communications with other federal agencies and local law-enforcement agencies to share information about possible threats. The communications plan should address all communication needs for annexes B through F above.

Annex J. A list of designated restricted, controlled, and utility areas.

Annex K. A list of installation MEVAs.

Annex L. A contingency plan. In most instances, it will be necessary to increase security for AA&E and other sensitive property, assets, and facilities during periods of natural disasters, natural

emergencies, or increased threat from terrorists or criminal elements. Therefore, Complains should include provisions for increasing the physical security measures and procedures based on the Installation/Depot Commander's assessment of the situation. Such contingencies may include hostage negotiations, protective services, and special-reaction teams. These provisions should be designed for early detection of an attempted intrusion, theft, or interruption of normal security conditions.

Annex M. CBRNE and Hazmat protection plan.

APPENDIX D: MAIL HANDLING AND SUSPICIOUS PACKAGES

A. General: This Appendix provides guidelines that may be adapted for opening mail and identifying and handling suspicious pieces. The safety of employees and the public is of paramount concern. These guidelines have been developed from the protocols and procedures recommended by the United States Postal Service. Each installation/activity/facility must continue its review of its mail operations and procedures.

1. The individual nature of each activity location should be considered in developing mail handling procedures. The size, layout, operational activities, emergency procedures already in place, etc., all need to be taken into account when reviewing and developing practical and effective mail safety procedures.

2. The objectives in any emergency mail handling procedures should include identifying and containing hazards, reducing their spread and preventing exposure.

3. Each activity should review and assess its procedures for handling mail, ensure if appropriate safety measures are being utilized and determine if any changes should be considered.

4. Emergency mail handling procedures should be incorporated in emergency and evacuation plans.

5. All outgoing mail must contain a return address.

B. Office Layout and Mail Operations. Where feasible, the mail opening activity should be situated in a specific office area, closed off if possible, to facilitate evacuation of the area with minimal disruption to other mail operations and public services.

C. Opening of Mail.

1. In order to avoid undue stress or needless concern, if there is something suspicious when inspecting and opening mail or packages, employees shall notify their supervisor before proceeding.

2. Examine unopened envelopes for foreign substances or powder.

3. Do not open letters with hands. Use a mail or letter opener, or scissors.

4. Open letters and packages with a minimum of movement to avoid spilling any contents.

5. Latex and non-latex gloves will be available for use.

D. Identifying Suspicious Mail. The following characteristics may identify a suspicious piece of mail. Common sense and logic should be used. One characteristic by itself may not necessarily mean an item is suspicious but should be taken into account when assessing the piece of mail. (see Figure D.1)

1. Any letter or package that has suspicious or threatening messages written on it.

2. Letters that have oily stains or are discolored or emit a peculiar odor.

3. Envelopes which are lopsided, rigid or bulky.

4. Envelopes with no return address and/or the sender is unknown. Envelopes with a suspicious return address.

5. Address is prepared to ensure anonymity of sender (e.g., labels, cut and paste lettering, poorly written, etc).

6. Unexpected envelopes from foreign countries.

7. Handwriting appears distorted.

8. Protruding wires or aluminum foil.

9. Excessive tape or string.

10. Postmark showing a different location than the return address.

11. Improper spelling of common words, names, places, or titles, or the name and title of addressee are inaccurate.

12. Markings such as "Personal," "Confidential," "Private," "Rush-Do Not Delay."

13. Personal mail when the addressee does not normally receive personal mail in the office. Note: Employees are prohibited from receiving personal mail at their work location.

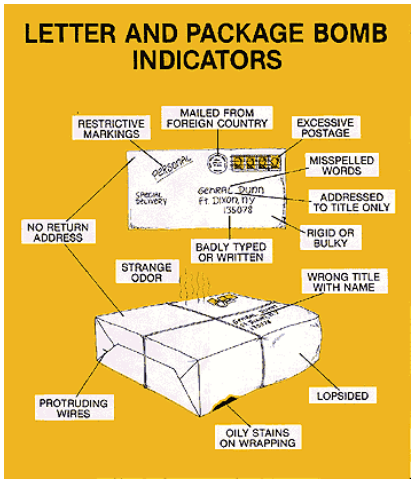

Figure D.1.

E. Handling Mail Identified as Suspicious.

1. If a mail item appears suspicious before or after opening, the handler should place the item aside, or in a plastic bag if one is available. No one should clean powder or other foreign substances.

2. The handler should not panic and should keep other employees away.

3. The handler should notify his or her supervisor. In addition, wherever there are security force officers on premises, they should be notified of a suspicious package or piece of mail.

4. For unopened packages or envelopes, the supervisor should immediately follow local notification procedures. If there is a spill after opening a suspicious package, then the supervisor should immediately call emergency response personnel (fire, police, medical).

5. The handler should not touch his or her eyes, nose or other parts of their body. If possible, he or she should wash their hands with soap and water. If clothing is contaminated, do not brush it at all. Steps such as cutting or removing contaminated clothing may be required. Remove and bag it at the site. The clothing should not be allowed to leave the area in order to avoid the potential of spreading any contaminant.

6. Employees and the public in the immediate vicinity must vacate the area. If possible, the room (doors and windows) should be closed off. Only qualified emergency personnel should be allowed to enter.

7. Turn off any fans or portable heaters.

8. Employees must go as a group immediately to the nearest vacant training/conference room or private office as instructed, preferably on the same floor. Employees must stay in this room together and not wander around the building in order that they can be identified for interview or later contact. Upon arrival, emergency personnel will provide additional instructions. If there is a "spill" in a public area, take the names and contact telephone numbers of anyone in that area that can be identified, then dismiss the members of the public.

9. Mail room staff will take direction from emergency personnel at the scene who will advise staff when it is appropriate to return to their work location.

10. No other area should be evacuated until directed by emergency personnel.

11. The area's heating, air conditioning and ventilation system should be shut off.

12. A list of people, who had actual contact with the powder or substance, as well as those in the area, should be made available for investigating authorities, including emergency and health officials.

13. As soon as the situation has been assessed, employees will be notified as to what action to take.

14. Any inquiries by the local press should be referred to the activity’s Public Affairs Office.

15. After the situation has been resolved and the office is back to normal, the office should complete and submit reports as required locally.

F. Removing Protective Gloves: Once gloves are contaminated, handlers must remember to only touch the outside of one glove to the outside of another glove, or other safe surfaces. Do not touch skin or clothing (see Figures D.2 – D.5).

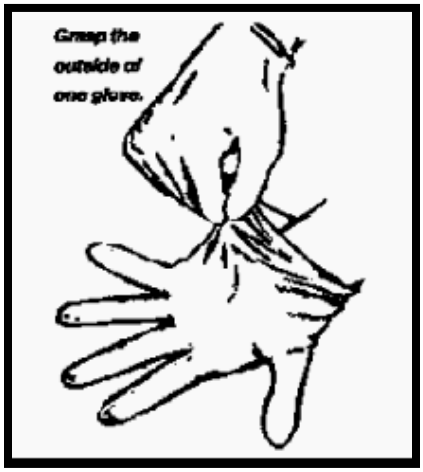

Figure D.2

Figure D.3

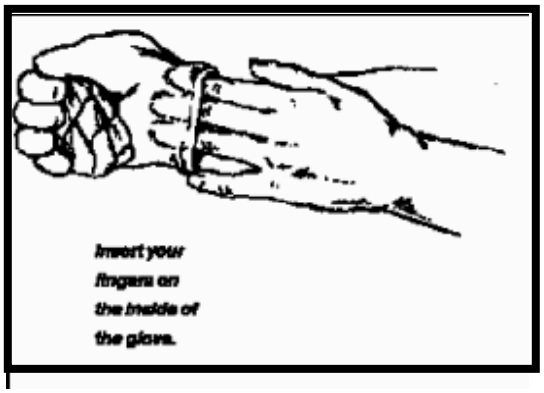

Figure D.4

Figure D.5

APPENDIX E: OPEN STORAGE INSPECTION CHECKLIST

OPEN STORAGE
INSPECTION CHECKL

APPENDIX F: OPEN STORAGE APPROVAL FORM

Open Storage Approval Form embedded as a fillable .PDF

DL1922, Request for
Open Storage Approv

The most current version is also available on the DLA Forms Program website at
http://www.dla.mil/dss/forms/

APPENDIX G: AA&E/ARMORY CHECKLIST

AA&E/Armory checklist.pdf

APPENDIX H: SURVEY AND INSPECTION CHECKLIST


dd2637-a.pdf


dd2637-b.pdf


dd2637-c.pdf


dd2637-d.pdf


dd2637-e.pdf


dd2637-f.pdf


dd2637-g.pdf


dd2637-h.pdf


dd2637-i.pdf

The most current checklist may be found here:
http://www.dtic.mil/whs/directives/infomgt/forms/dd/dd2637.htm

APPENDIX I: REQUEST FOR DEVIATION FROM SECURITY CRITERIA APPROVAL FORM (DL1885)

Request for deviation from securit

The most current version is also available on the DLA Forms Program website at http://www.dla.mil/dss/forms/